Solution Sheet

Regaining Control Over ActiveX

ActiveX security risks are widespread and traditional IT management tools can't track and secure this browser technology.

Problem

Many critical business applications rely on ActiveX, a powerful, yet inherently unsafe, browser technology. In the past, business needs have routinely outweighed the security risks, so IT allowed ActiveX controls to be installed and run with little oversight. This lack of urgency in addressing ActiveX security has caused this problem to become larger and more widespread over time. The problem has been compounded by the lack the IT management tools required to assess and remediate ActiveX.

Legacy business applications continue to power your daily business operations, and those critical web applications rely, in part, on ActiveX. Efforts to replace and modernize core business applications take time, testing, and planning. In the meantime, your organization must let them continue to run. Over time, you've had to make security versus functionality decisions, many of which have left your entire enterprise at risk. You're in good company. Most organizations long ago lost track of which web applications needed which ActiveX controls, what security risks they agreed to live with, and what settings were deployed in an attempt to mitigate those risks. Now the problem is too big and broad and too high risk for any enterprise to remain complacent. And traditional desktop management tools are not equipped to help you get back on track. A new solution is required.

Solution

Browser management is the key to ActiveX inventory, usage tracking, and secure deployment.

Logic dictates that you can't manage what you can't see. So the first step toward regaining control over ActiveX is discovery – compiling a complete and robust inventory of your environment. Most organizations rely on traditional desktop management tools to collect inventory data from end user systems, but those tools only provide raw installation data. This data, without context, is meaningless. The key to turning your inventory data into useful information is gaining the ability to correlate the data with actual web application usage by individual end users. Only then can you plan a proactive remediation path.

ActiveX has a longstanding reputation for being insecure, so many organizations like yours are eager to eliminate it. Often times that process is stymied by the mere fact that your organization doesn't know what web applications and ActiveX controls you have, and where they are used. Even if your organization has perfect information on business needs with regard to the dozens of ActiveX controls found on each of the thousands of PCs in your enterprise, you can't simply eliminate them overnight. Building and deploying new systems to

replace the applications reliant on this legacy technology will take time and money. Inevitably, your new systems won't just be direct replacements because the business will request new features and functionality, extending the time and cost of development. All the while, ActiveX security risks remain and your business is exposed.

Not all ActiveX security threats are equal. If your organization has made compromises with ActiveX security to enable a seamless business workflow, the dangers can be worse. By reducing the ActiveX security posture for those business scenarios, your organization has increased its risk. As is typical, you likely have few, if any, records of which "known unsafe" controls are needed where, compounding the problem and making the solution seem out of reach.

Browsium's innovative browser management suite enables organizations to regain control while enforcing greater security for ActiveX controls. Securing ActiveX starts with discovery – using the inventory and analysis power of the browser management suite to build a complete, correlated, and comprehensive inventory of your web application estate. The key is not just looking at ActiveX, but assessing the entire web application platform to fully understand what is needed, where it's needed, and when it's needed. From there, your organization has the information (not just the data) to make a plan for effective ActiveX management that meets the needs of both IT security and your business. Lastly, the browser management suite has the tools to act on those decisions and deploy rules to enforce behaviors. What's more, with the full suite in place, your organization now has an end-to-end system in place so you'll never be left in the dark again. Your browser blind spots will be eliminated, and end user management can become a reality in your web application environment.

How to get started

Browsium's browser management suite is comprised of three software modules: Browsium Proton, Browsium Ion, and Browsium Catalyst. Together this solution allows you to discover, plan, and act to proactively manage your mission critical web application environment.

Don't wait any longer to take control of ActiveX and improve security in your enterprise. Start by planning a **Browsium Browser Management Assessment** in your organization. This two-week program will use your data to shed light on the browser blind spots in your environment that expose you to some unexpected risks. Learn more by visiting http://www.browsium.com/assessment-program/ or email us at info@browsium.com.

Browsium, Inc.
8201 164th Ave. NE, Suite 200
Redmond, WA 98052
www.browsium.com
+1.425.285.4424