Carbon Black.

Cyber Compliance

Grahm Leach Bliley Act (GLBA)

Using Carbon Black to help achieve GLBA compliance

October 2018

Executive Summary/Highlights

The Gramm-Leach-Bliley Act of 1999 (GLBA) was enacted to modernize the financial services industry by removing regulations that prevented the merger of banks, stock brokerage companies, and insurance companies. In the spirit of modernization, the federal banking agencies and the CFTC, FTC, NCUA, and SEC issued Title V, entitled "Disclosure of Nonpublic Personal Information (NPI)" to institute privacy policies that would protect customers and consumers NPI. Additionally, within the GLB Act, the Federal Trade Commission (FTC) enacted the Safeguards Rule, which requires financial institutions under FTC jurisdiction to have proper controls in place to keep customer information secure.

Title V - Privacy Rule:

The Privacy Rule requires financial institutions to notify both customers and consumers of the policies that are in place to protect their confidentiality, as well as, how the financial institution secures that information.

Safeguards Rule:

The Safeguards Rule requires organizations to assess and address the risks that threaten the safety of customer information in all areas of operation. Three areas that are particularly important to information security are Employee Management and Training; Information Systems; and Detecting and Managing System Failures.

Nonpublic Personal Information - Personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution."

Who must Comply with GLBA?

GLBA has been around in its current form some time now, but there continues to be confusion regarding who must comply. Part of the problem is that the term "financial institution" is somewhat vague. Listed below is a breakdown of businesses deemed financial institutions.

Beyond just banks:

+ Non-depository lenders, Consumer reporting agencies, Data processors, Courier services, Retailers that extend credit by issuing credit cards to consumers, Personal property or Real estate appraisers, Check-cashing businesses, and Mortgage brokers.

Higher education institutions:

+ The GLBA Safeguards Rule has always applied to higher education institutions, but the Department of Education historically did a poor job of communicating this expectation to the institutions.

+ In 2016, the DOE reiterated that higher education institutions must comply with the Safeguards Rule and those who do not risk losing a school's Title IV funding. Additionally, the DOE expects to have the Safeguards Rule included as testing criteria in the 2019 release of the Office of Management and Budget Compliance Supplement for external auditors to follow when testing the Student Financial Assistance cluster.

Accounting Firms:

+ Identity thieves and hackers are increasingly targeting certified public accountants due to the highly sensitive personal information they store.

+ The IRS warns that some tax professionals may be unaware they are victims of data theft, even long after digital intruders have stolen all of their clients' data.

Hospitals:

+ While hospitals are well aware of HIPAA regulations, the same can not be said for their acknowledgment that they too are considered a financial institution.

+ Why is a hospital considered a financial institution? Look at how the hospital bills its patients. If the hospital provides long-term payment plans with interest, then GLBA is now a reality.

3 fundamental areas to GLBA Success:

Within any successful cyber regulatory program its important to remember that technical controls are only effective when they are a part of a healthy information systems risk management program. GLBA requirements are a mix of technical and governance. Carbon Black helps enterprises in each of these three fundamental pillars.

1. **Institute a comprehensive information security program.** There is no silver bullet that guarantees GLBA compliance. To reach a satisfactory level of compliance, you need in-depth understanding of what data you control, precise privacy policies and the ability to identify when there's been a breach. One way to create this program is by piecing together different solutions that check the box for compliance. Alternatively, Carbon Black's Predictive Security Cloud offers many controls through a single pane of glass. When you show customers you care about the security of their personal information, you increase their confidence in your company.

2. **Visibility.** The Carbon Black Predictive Security Cloud platform introduces a powerful set of technologies delivered from a single agent and a single console. With the Carbon Black Predictive Security cloud platform we are delivering a better security solution based on the experience of our founding team who were trained as offensive hackers by the NSA and CIA. Their fundamental insight was that the only way to see and stop the adversary is to collect the most complete data and to apply the best analytics to that data.

3. **Endpoints are the new permiter.** Endpoint devices represent the new parameter that must be protected. In today's new reality, the device, and the people operating those devices, have taken center stage. Whether in your office or at a Starbucks, your endpoints now have access to some of your organization's most sensitive data via cloud services, such as Salesforce.com, Office 365, and the Google Suite. This makes it extremely important that each endpoint has its own perimeter able to defend against the most advanced modern attacks.

Carbon Black.

Cb Predictive Security Cloud™

Cloud-Based Endpoint Security

Enterprises today currently have on average over 70 different security vendors deployed within their networks and they are looking to consolidate. Cb Defense the flagship product on the PSC combines NGAV and EDR from a single agent.

On top of Cb Defense, Carbon Black offers Threatsight, our managed threat hunting service. Threatsight adds a layer to the continuous validation of security controls as required by GLBA.

Carbon Black's unique approach is to leverage the power of our unfiltered data and our streaming analytics to provide the full security life-cycle, that is to prevent, to detect, and to respond to current attacks and to predict future attacks.

GLBA Compliance Use Cases

- Validation proof of AV certification
- File Integrity Monitoring & File Integrity Control
- Lock down critical systems and applications
- Protect fixed-function devices
- Secure virtual datacenters
- Pre-compliance gap and data gathering on endpoints.

Beyond Compliance

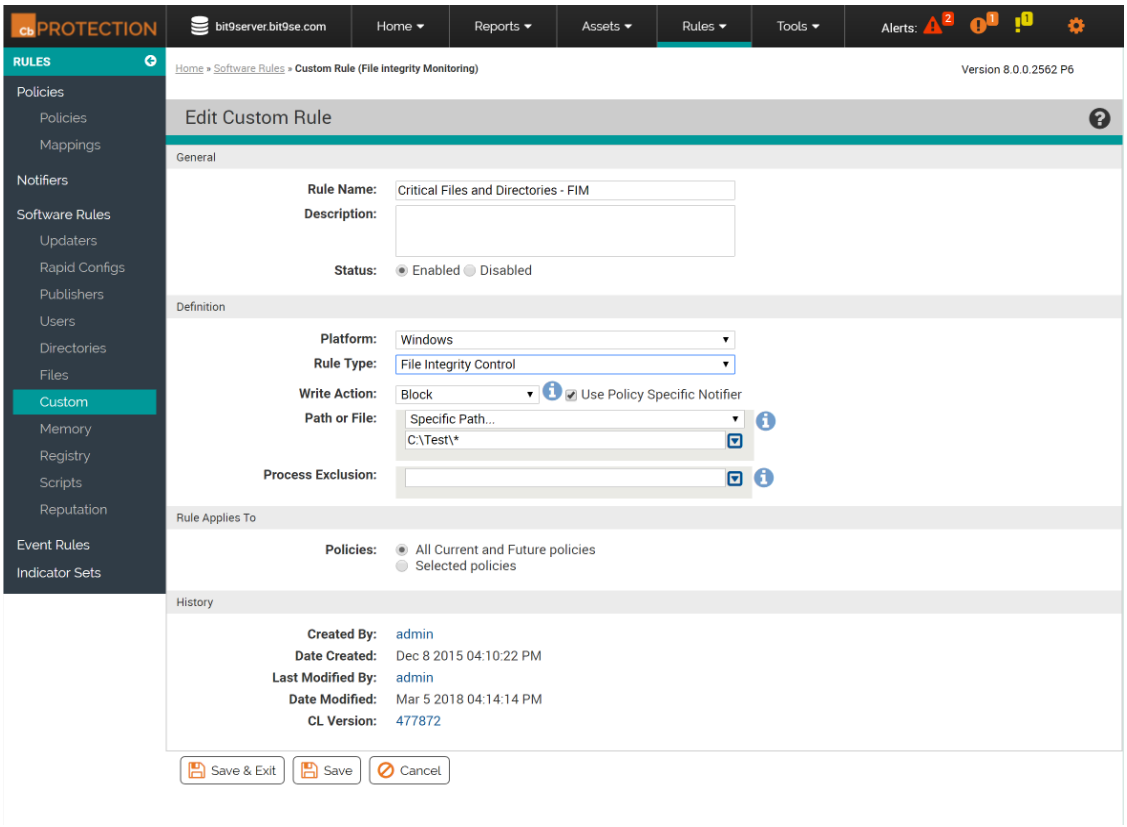
- Cb Defense can block or detect malicious activity including, memory scraping, lateral movement, credential theft, persistence, command & control communication and more.
- The EDR capabilities baked into CbD keep endpoint configurations in check by finding vulnerable applications in the enterprise, and identifying if a vulnerable application has ever been seen, when it was last seen, and on which computers.
- When an endpoint exhibits malicious behavior, Live Response allows admins to directly access the machine through a secure remote shell to perform further investigations and remediate the issue.
- Cb Defense collects and transmits all unfiltered data in real-time to the Cb Predictive Security Cloud. By applying streaming analytics to that data, consisting of behavioral analytics, machine learning, reputation scoring and real-time signature analysis, CbD goes beyond traditional antivirus and even machine learning AV to predict threats never seen before.

Carbon Black.

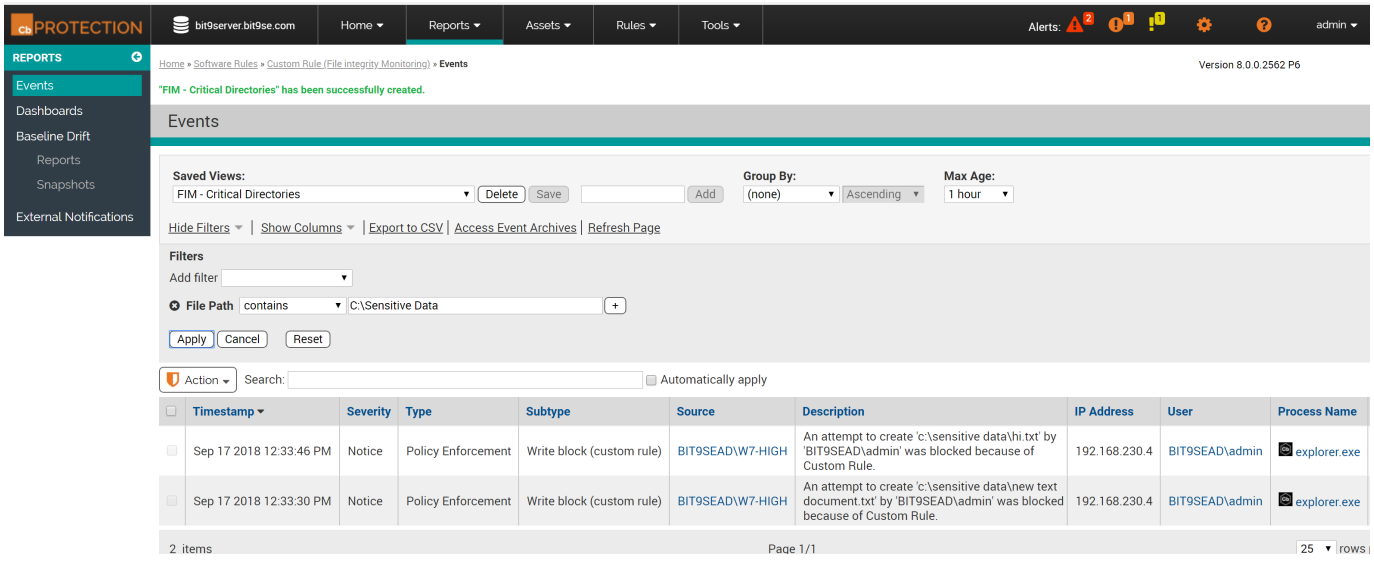
Simple & Powerful Examples:

Below are screenshots with brief descriptions of how Carbon Black can provide coverage for key GLBA requirements.

Configure File Integrity Monitoring rules – Define critical files or file paths. Specify Process exclusions for expected changes.



Saved Views for FIM Critical Directories includes User and Process that made changes. Providng, the recording and retaining of details for when changes were made.

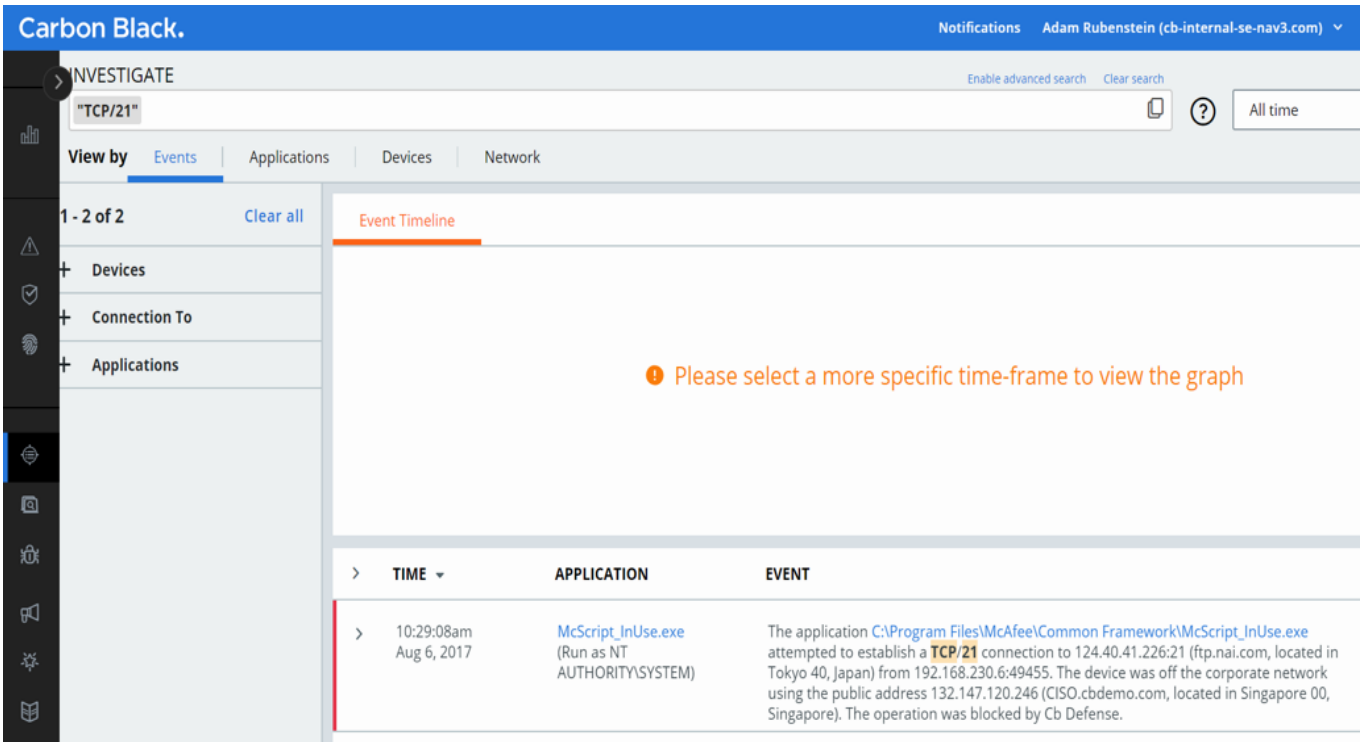


Identify Insecure Services - Where possibly these services and the related protocols should be disabled. It was common in the past seeing protocols sharing authentication credentials and other sensitive data, without any form of encryption. This does not make the protocol itself insecure, yet makes data susceptible for capturing by unauthorized parties. This results in an insecure service, which needs careful consideration when being used or implemented.

Example 1 - With CbD you can investigate layer 4 traffic with the protocol and port number of a network connection. i.e. “TCP/21” for FTP

Examples of commonly seen unencrypted protocols, plus their secure alternatives:

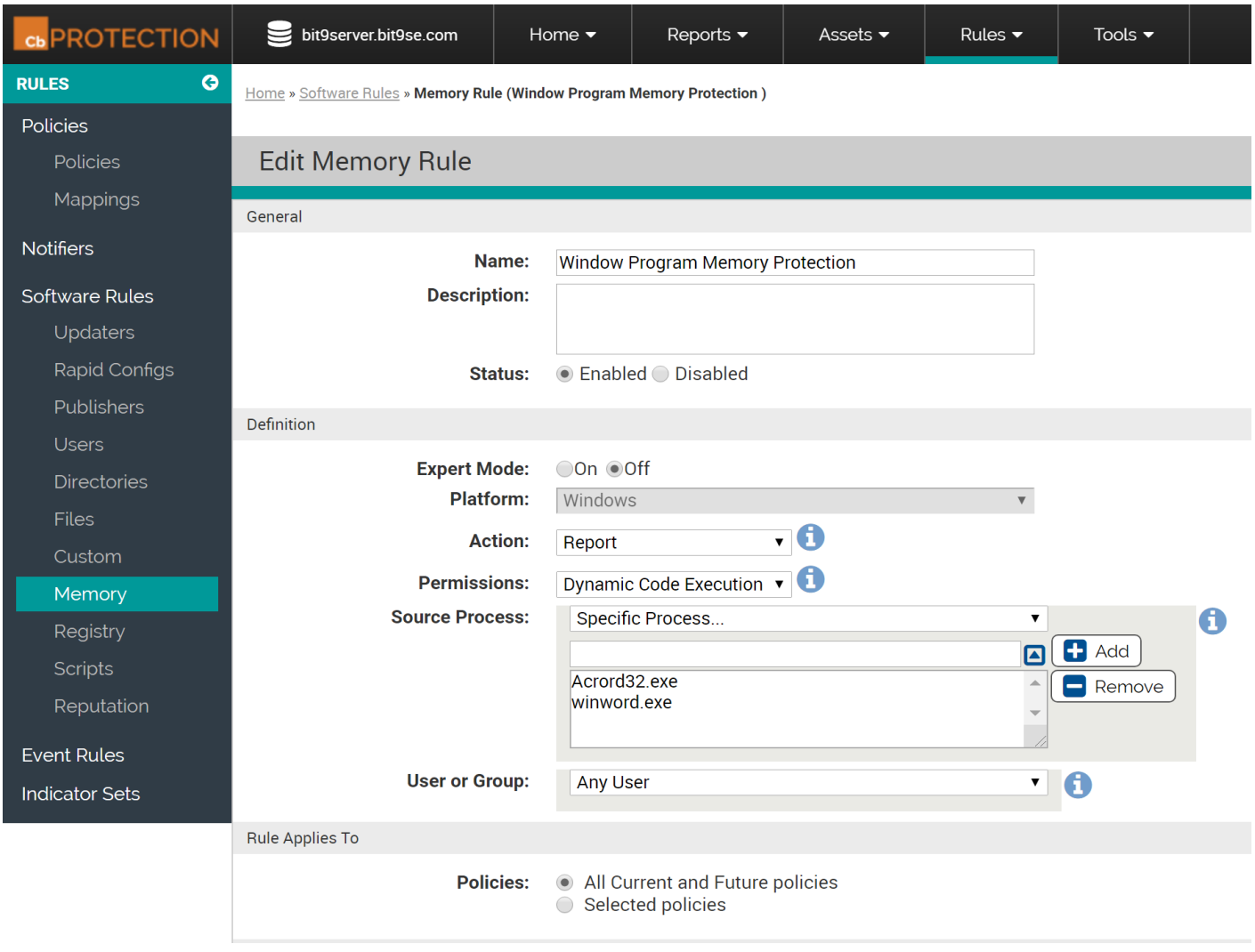
- FTP (FTPS, SFTP, SCP)
- HTTP (HTTPS)
- IMAP (IMAPS)
- POP3 (POP3S)
- SNMP v1/v2 (SNMP v3)
- Telnet (SSH, Mosh)



Carbon Black.

Implement safeguards to protect memory from unauthorized code execution

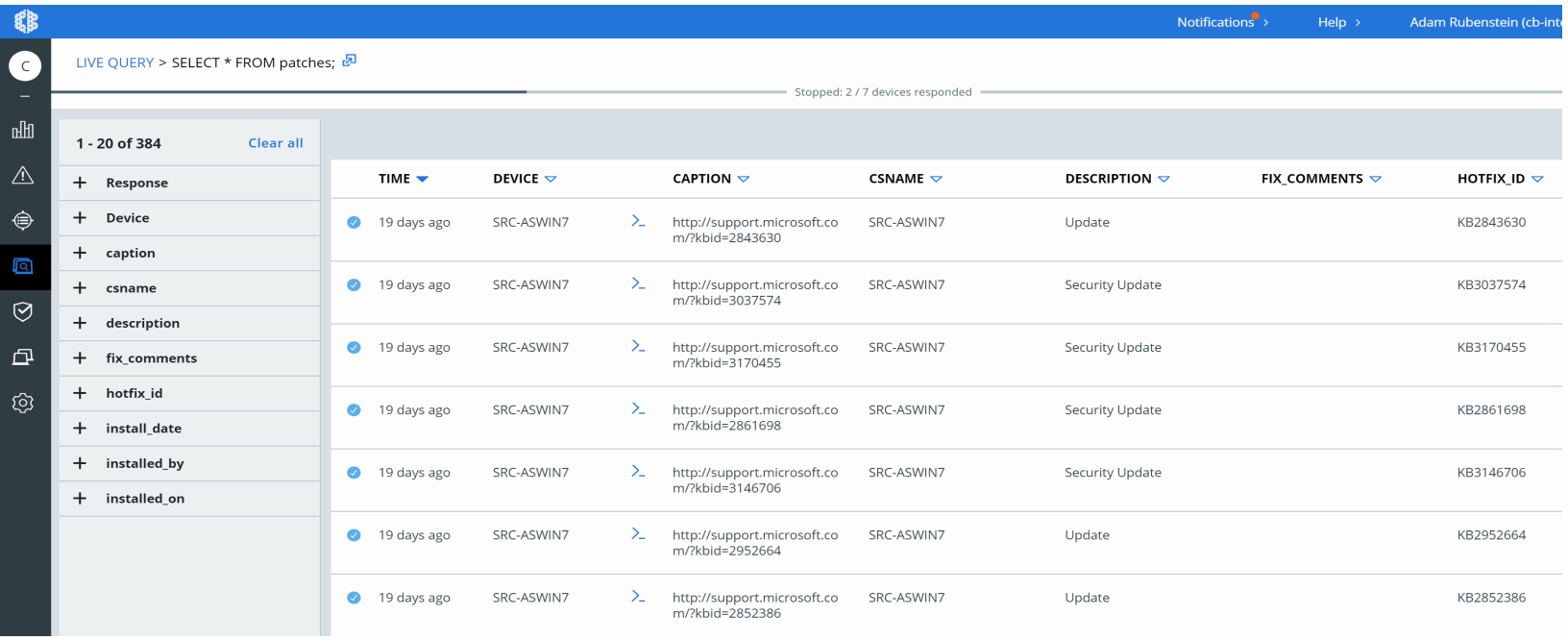
Dynamic Code Execution, affects whether an application can execute code not associated with an executable image. This protection prevents arbitrary or floating code execution used by many forms of malware, ultimately preventing any unauthorized code from executing and effectively blocking the secondary stage of many attacks.



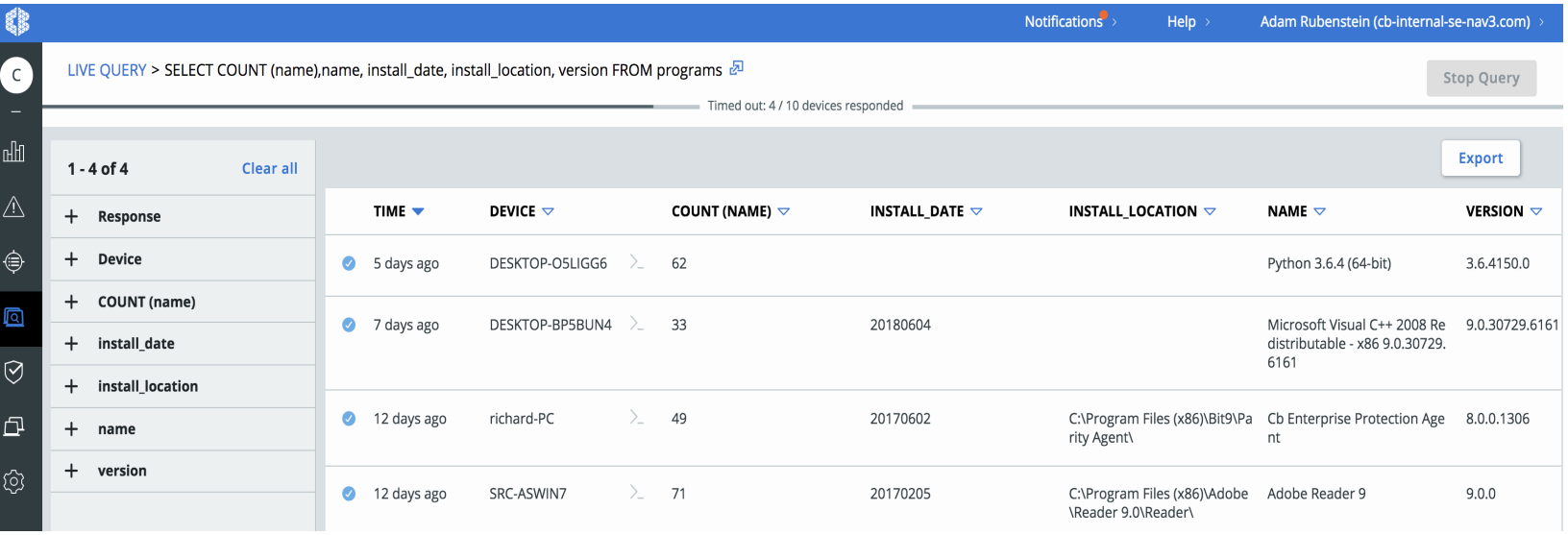
Carbon Black.

Live Query keeps your systems and devices in compliance. If you find out that a program update is required due to a known vulnerability, you can simply scan your organization for any devices running the old version, and either let the owners know, or implement the update yourself using Live Response.

This simple query lists all patches applied, with the column HOTFIX_ID representing the KB ID of the patch.



Identify applications by name that are installed on your endpoints. With the added details of install date, the directory of installation and the product version information.



Carbon Black.

1100 Winter Street, Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499

carbonblack.com

ABOUT CARBON BLACK

Carbon Black is the leading provider of next-generation endpoint security. With more than 13 million endpoints under management, Carbon Black has more than 3,000 customers, including 30 of the Fortune 100. These customers use Carbon Black to replace legacy antivirus, lock down critical systems, hunt threats, and protect their endpoints from the most advanced cyberattacks, including non-malware attacks. For more information, please visit www.carbonblack.com or follow us on Twitter at @CarbonBlack_Inc.