ExtraHop

Security Advisory

IS YOUR ENTERPRISE DATA BEING “PHONED HOME”?

Enterprises rely on third-party vendors for everything from infrastructure and applications to security, but they often don't know how those vendors are using their data. In this Security Advisory, we discuss four real-world examples of data being "phoned home" and share best practices for ensuring data security, privacy, and compliance.

REPORT INTRODUCTION

Security and IT organizations seldom realize how often and in how many ways their data is sent by vendors to vendor environments. This report provides four real-world examples of vendors "phoning home" data in an unauthorized manner, observed by ExtraHop customers in 2018 and the first weeks of 2019. The report also discusses the legal and regulatory implications of this data exfiltration, as well as recommended remediation actions and questions that customers should ask vendors.

Example 1

Endpoint security vendor sending data to the cloud after evaluation has ended

Organization type	Financial services provider
Vendor type	Endpoint security
Activity	Sending encrypted traffic to the public cloud after an evaluation had ended
Risk	Unauthorized access to data
Recommended Actions	**1.** Track deployment of software agents deployed as part of an evaluation **2.** Monitor egress traffic, especially from sensitive assets such as domain controllers **3.** Monitor for vendor activity post-evaluation

Example 2

Device management vendor sending data to the cloud

Organization type	Hospital
Vendor type	Device management
Activity	Sending data to the cloud without authorization
Risk	Potential HIPAA violation requiring incident response
Recommended Actions	**1.** Match egress traffic to approved applications and services **2.** Track whether data is used in compliance with vendor contract agreements

Example 3

Unauthorized security camera facilitating potential malware downloads

Organization type	Food services provider
Vendor type	Consumer security camera
Activity	Sending data to a known malicious IP address located in China that hosts malware
Risk	Potential vector for malware downloads
Recommended Actions	**1.** Consider requiring network authentication to block unauthorized IoT devices **2.** Monitor egress traffic across all devices connected on the network **3.** Track outbound connections to suspicious IP addresses and geographies

Example 4

Security analytics vendor phoning data home over geographic and political boundaries

Organization type	Financial services company
Vendor type	Security analytics
Activity	Sending more than 1 TB of customer data from the United States to vendor servers in the United Kingdom
Risk	Potential exposure of PII and violations under Gramm-Leach-Bliley Act
Recommended Actions	**1.** Match egress traffic to approved applications and services **2.** Track whether data is used in compliance with vendor contract agreements **3.** Understand regulatory considerations of data crossing political and geographic boundaries

Is Your Enterprise Data Being Phoned Home?

Introduction

On the heels of the many recent privacy scandals, the manner in which companies handle and use customer data has been the subject of much scrutiny, including Congressional hearings on the matter. Practically every company a consumer interacts with, whether it's Facebook, Google, or otherwise, is not only using customer data, but in all likelihood sharing it with third parties as permitted under their terms of service.

But consumers aren't alone in needing to worry about how companies are using their data. Enterprise organizations put massive volumes of data into the hands of third-party vendors. In some cases, like SaaS applications, it's explicit that enterprise data will live within a third-party environment. With other products, particularly those that live within the enterprise data center or cloud infrastructure, exactly how much data those vendors "phone home" to their own environment for things such as analysis can be a lot less clear. When you factor in the devices that employees themselves connect to the network without the knowledge of IT, knowing exactly how, when, and for what purpose third-party vendors are using your data can be exceptionally difficult.

What is "Phoning Home"?

From our vantage point of seeing everything that happens on an enterprise network, we see a frequent pattern of vendors "phoning" or "calling" data home (the white hat term for exfiltrating data) to their environments. To be clear, phoning data home is not problematic at face value. Vendors, including ExtraHop, phone customer data home for a variety of perfectly legitimate and useful reasons with the customer's advance knowledge and approval, and do so securely through de-identification and encryption.

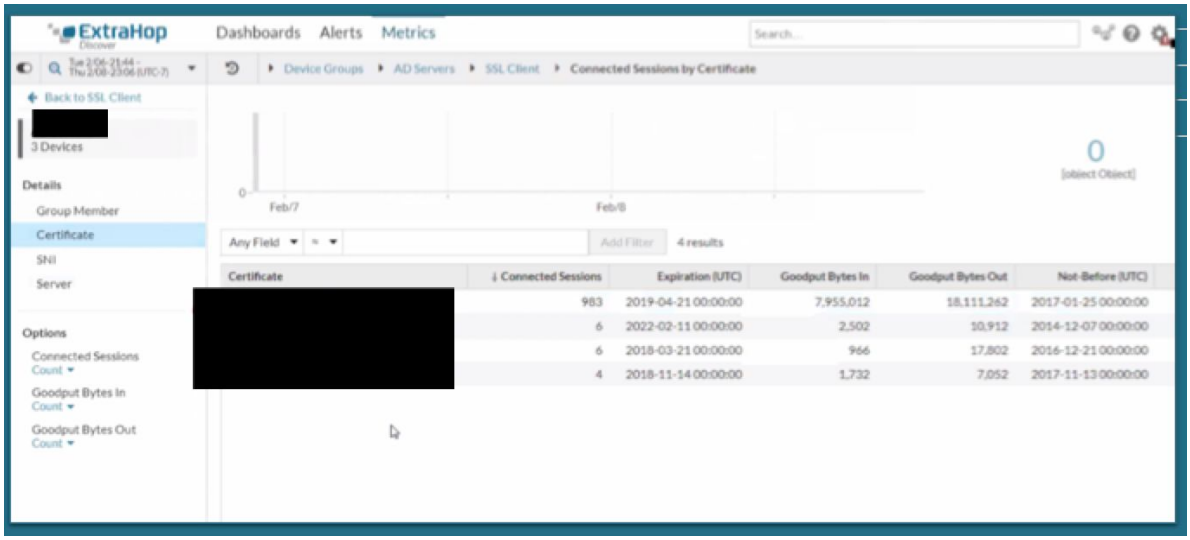
But phoning data home becomes problematic when enterprise customers are unaware that certain sensitive data (like Personally Identifiable Information [PII]) is leaving their environment, or the vendor is phoning home data at all. And it's a lot more common than you'd think. Below are four scenarios documented by ExtraHop in customers' production environments in 2018 and the first weeks of 2019.

Case Study 1

Good connection? That's not a good thing.

Sometimes training sessions with customers unearth very interesting discoveries. During a recent session with a customer in the financial services industry, the ExtraHop trainer noticed that domain controllers were shipping data to a public cloud instance. The customer's immediate reaction was "that's not possible."

But not only was it possible, it was happening. Domain controllers were sending SSL traffic outbound to 50 different public cloud endpoints.



A glance at the certificate revealed another well-known vendor was phoning data home to a cloud storage instance in vendor-owned IP space. The problem? This wasn't actually one of their vendors. The financial services company had evaluated the vendor's product months earlier but didn't buy. All vendor connections were supposed to have terminated when the proof of concept (POC) ended, but outbound traffic continued for at least two months.

This example should be of particular interest to enterprises. According to some estimates, the average medium to large enterprise has anywhere from 300 to over 500 cloud applications in use. Many of those were not officially sanctioned or deployed by IT, and many don't include important safeguards such as encryption for data at rest. In light of this, it's more important than ever for enterprises to understand which cloud apps are accessing company data, how they are using that data, and where those apps are sending the data.

Case Study 2

“The bucket better not be open!”

Another example of phoning home took place in a hospital located in the Western United States. The hospital was piloting a medical device management product that manages phones and tablets loaded with appropriate medical apps and patient info for medical staff. The devices were able to be used only on designated hospital WiFi, making it difficult for any data to leave the device unless it’s being sent over the hospital’s own secure connections. This practice is excellent for ensuring HIPAA compliance and generally protecting patient data.

One afternoon a member of the security team noticed that traffic from the workstation managing the initial device rollout was opening encrypted SSL:443 connections to vendor-owned cloud storage. Given the spate of recent incidents in which public cloud storage had been left open to the internet, the security analyst’s first reaction was, “What data are they pushing, and why?”

For hospitals and other healthcare delivery organizations subject to HIPAA, understanding who has access to potentially high value data is critical. Until they spotted the exfiltration in the network traffic, the hospital security and IT teams had no idea that the device management company was phoning home any data, how they might be using it, or how long it had been going on. Under HIPAA, an incident such as this typically requires significant documentation, as well as incident response and cleanup.

Case Study 3

When Shadow IT Phones Home

Recently ExtraHop was on-site with a large multinational food services company. During the data review, the customer noticed that approximately every 30 minutes, a network-connected device was sending UDP traffic out to a known bad IP address. The activity was taking place during normal working hours. As it turned out, the device in question was a Chinese-manufactured security camera—likely set up independently by an employee at their office for personal security purposes. The camera was phoning home to a known nefarious IP address with ties to China.

In order to understand how this was happening, the team at the food services company connected to the device via a web browser and was instantly prompted to download an executable file. When the employee who installed the camera connected it to the company's network, they would have also been prompted to download the potentially malicious executable, unknowingly exposing the company to exfiltration of data.

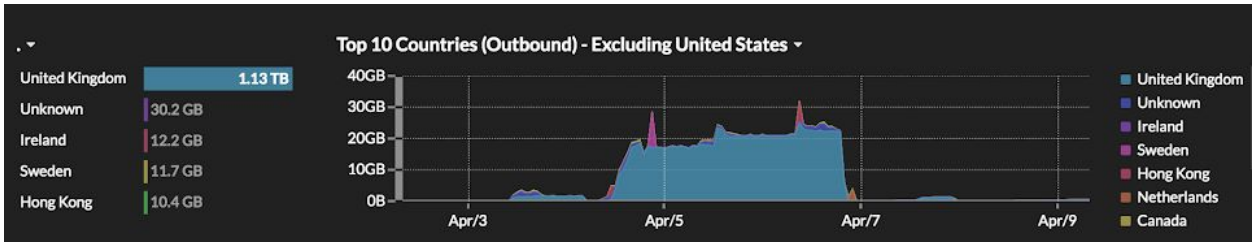
The irony of this particular story is clear. An employee, concerned about the security of their office, installed an unauthorized camera that then proceeded to maliciously exfiltrate data to a known bad actor. Unlike the other examples captured in this report, this story doesn't involve an approved vendor engaging in unapproved behavior, but it does underscore the ubiquity of this type of behavior, and how well-known consumer brands can expose an enterprise to risk.

Case Study 4

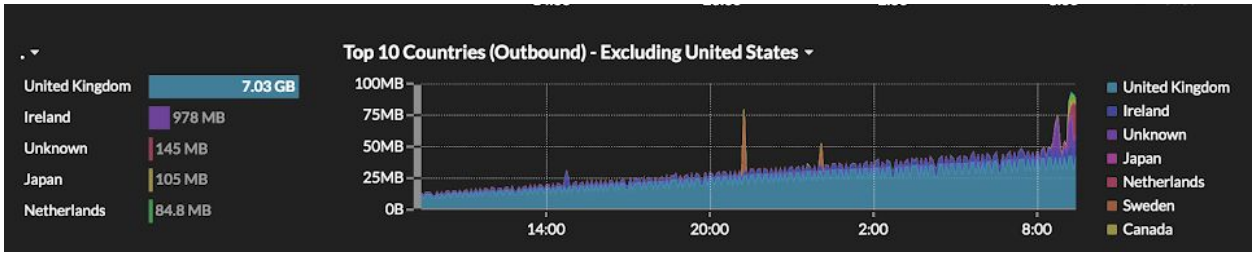
When "on-box analysis" isn't entirely "on box"

During a recent POC with a large financial services institution in the U.S. Midwest, ExtraHop noticed a large volume of outbound traffic headed from the customer's U.S. datacenter to the United Kingdom. Right away, this particular instance of phoning home was problematic for a few reasons. First, the customer was unaware that any data was leaving their environment. Second, the data was crossing geographic and political boundaries—which can be problematic if not done properly under data compliance regimes like the Gramm-Leach-Bliley Act (GLBA) and GDPR.

Closer examination of the traffic—more than 400 GB of data per day over two-and-a-half days (totaling more than 1 TB)—revealed that it was a security technology vendor that was also in a POC with the financial services institution at that time. For the sake of comparison, watching a Netflix movie requires about 3 GB per hour.



The traffic pattern itself was also concerning. While large volumes of data were being phoned home during regular business hours, the traffic exfiltration tapered off around close of business in the United Kingdom on Friday, and then picked up again early Monday morning, indicating a human-directed component to the behavior.



While it's certainly not unheard of for security vendors to phone home data, the customer was surprised to see this vendor engaging in this practice because the vendor claimed to perform all analysis and machine learning on-box—meaning on the appliance deployed in the customer's environment. Such a configuration should preclude the need to phone data home.

Whether due to a configuration error or some other benign purpose (such as secondary analysis), seeing data exfiltrated without their knowledge across geographic boundaries by a trusted vendor was a wake-up call for the financial services institution.

So what's really going on?

To be clear, we don't know why these vendors are phoning home data. The companies are all respected security and IT vendors, and in all likelihood, their phoning home of data was either for a legitimate purpose given their architecture design or the result of a misconfiguration.

But the fact that large volumes of data are traveling outbound from a customer environment to a vendor without the customer's knowledge or consent is problematic. That some of the traffic is going into cloud storage space (which is at the center of several notorious data breaches that together account for more than 70 percent of lost records in 2017), is even more troubling.

What these examples underscore is that it's very difficult for enterprises to really understand what's happening with their data. How can you expect to know when a bad actor is exfiltrating data when you don't know that your trusted vendors are pulling it out of your environment and for what purpose?

A regulatory headache

Although the United States doesn't have a unified data privacy framework, many large enterprise organizations operate according the General Data Privacy Regulation (GDPR). Depending on industry, they may also be subject to other data security or privacy regulations such as the new California CCPA, HIPAA, PCI, GLBA, FISMA, etc.

These regulations, GDPR in particular, require that organizations know exactly what data they have, the value of the data, how they are using it, and how they are protecting it. If an organization is

unaware that a vendor is removing data from their environment, no matter how benign the reason, it eliminates that certainty. How can you implement a privacy program if your vendors are doing things with your data that you don't know about?

This also gets at the heart of the processor/controller relationship. In many cases, an enterprise may be both a controller and a processor. As a controller, enterprises must only appoint processors that guarantee compliance with GDPR. If an enterprise has no way of knowing what a vendor is doing with the data, then the enterprise cannot lawfully appoint the vendor and would risk penalties in doing so anyway.

For organizations that fall into the processor category (and most do with respect to at least some of their data), any data phoned home by a vendor, even for a benign purpose, makes that vendor a sub-processor. If the organization is unaware the data is being phoned home, they are still responsible for the sub-processor's actions and may be exposed to additional liabilities.

In the Interest of Transparency, a Bit of Context

The ExtraHop platform was engineered from the beginning for privacy and security. Our products passively monitor and analyze all network traffic, which includes every single digital interaction between every system on the network. If two devices or applications communicate with each other, even once, we see it. With that information, we surface everything from performance degradations to security threats to abnormal traffic patterns.

Our machine learning took years to create, continues to evolve, and plays a critical role in threat detection and investigation. In order to take advantage of scalable computing resources in the cloud, our machine learning is performed in the cloud rather than on-box in the customer's environment. The fact that our machine learning service is based in the cloud is a competitive advantage, giving our product access to nearly infinite memory and compute resources. For example, we use these resources to build more than 100 predictive models for each entity we observe, such as an asset, IP address, or user. In an environment with 10,000 entities, that's more than a million individualized machine-learning models!

ExtraHop phones home a limited subset of de-identified customer metadata for analysis performed in a dedicated cloud instance in the customer's geographic region, and we inform the customer up front that this is happening. We strip the de-identified metadata of all identifying information including IP addresses, user names, file names, etc. We also encrypt the data using a customer-held key. Anomalies and security events are then sent back to the customer environment, where they are re-identified and decrypted with the customer-held key, for alerting and investigation. We do not phone home data unless explicitly authorized by the customer to do so.

Mitigating the Risks of Unauthorized Phoning Home

In addition to the remediations outlined in this advisory, ExtraHop urges companies to ask questions of their vendors to ensure they understand how their data is being used. Enterprises should know where their data is going and understand vendors' protocols for phoning data home.

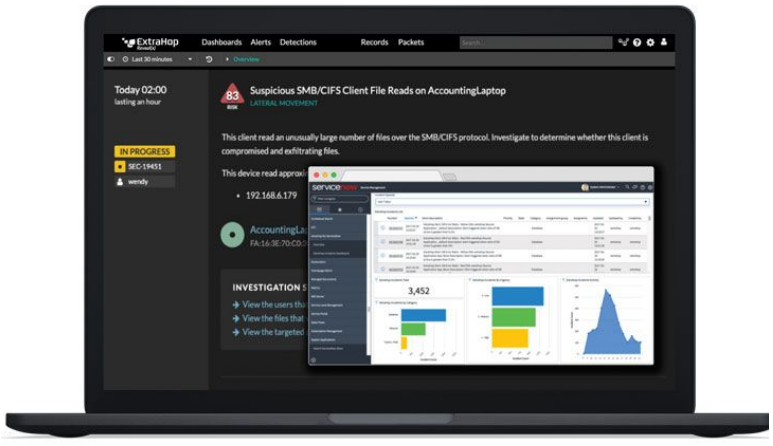
These actions will hold vendors more accountable and will ultimately limit the exposure of sensitive enterprise data that can be associated with phoning home.

Sample Questions for Vendors

- Are analytics performed locally in the customer environment or in the vendor environment?
- If data is moved outside the customer environment, does that include PII?
- If the vendor phones home data, are they handling it in an environment and manner that is compliant with the applicable regulations?
- Cryptographic protocols that utilize perfect forward secrecy will more effectively protect data that is captured in transit. What level of encryption does the vendor use to protect customer data in transit?
- What other measures are in place to ensure that customer data is protected?
- How are connections to the customer environment terminated, and how is that communicated to the customer?
- Is data segmented by customer or comingled in the vendor environment?
- Has the vendor undergone a third party audit? Penetration tests? Does the vendor meet regulatory requirements relevant to your industry? Do they have any certifications?

Meet Reveal(x)

The integrated Reveal(x) approach accelerates enterprise programs, reduces errors and duplicated effort that come with one-off and siloed decision-making, and minimizes disruption and risk from tool false positives. Get started today in taking your enterprise security and operational preparedness to the next level.



Learn more about our current partners, integrations, and APIs available at
www.extrahop.com/integrations

ExtraHop demo online at
www.extrahop.com/demo

ABOUT EXTRAHOP NETWORKS

ExtraHop provides enterprise cyber analytics that deliver security and performance from the inside out. Our breakthrough approach analyzes all network interactions and applies advanced machine learning for complete visibility, real-time detection, and guided investigation. With this approach, we help the world's leading enterprises rise above the noise of alerts, organizational silos, and runaway technology. Whether you're investigating threats, ensuring delivery of critical applications, or securing your investment in cloud, ExtraHop helps you protect and accelerate your business.