Endpoint Security through Device Configuration, Policy and Network Isolation
Abstract

Sensitive data leaked from endpoints unbeknownst to the user can be detrimental to both an organization and its workforce. The CIO of GIAC Enterprises, alarmed by reports from a newly installed, host-based firewall on his MacBook Pro, commissioned an investigation concerning the security of GIAC Enterprise endpoints.

The study has the following objectives: 1) to analyze and increase the security of ‘known’ employee endpoints; 2) to increase safety of employee and contractor endpoint devices; and 3) to guard against loss of GIAC competitive edge due to information unknowingly leaked from endpoints. This report reviews the findings and provides several recommendations on how GIAC Enterprises can improve the security around their endpoints and the protection of sensitive data through device configuration, policy, and technical improvements to key workflows.
1. Executive Summary

A simple request, a complex set of answers. This project started with a simple request from the CIO of GIAC Enterprises, a request to understand what information was being sent from the endpoints within the organization without user knowledge and what risk this posed to the organization and its workforce.

We started with three objectives:

- **Objective One**: Increase the security of ‘known’ employee endpoints
- **Objective Two**: Increase safety of employee and contractor endpoint devices
- **Objective Three**: Guard against loss of GIAC competitive edge due to leaked information from endpoints

We found lots of detail related to each goal, but we identified this set of five recommended actions to improve the GIAC security posture around endpoints and sensitive data,

- **Recommendation 1**: GIAC employee endpoints need stronger controls to minimize the data provided to third parties.
- **Recommendation #2**: GIAC should deploy a new cloud-based architecture for submittal and translation of fortune saying to reduce the security concerns around unmanaged contractor endpoints.
- **Recommendation #3**: GIAC should develop a policy and process for the approval and management of apps authorized for installation on corporate devices.
- **Recommendation #4**: GIAC should evaluate the corporate need for IP address masking and obfuscation.
- **Recommendation #5**: GIAC should create and provide user training on the protection of sensitive information.
2. Introduction

GIAC Enterprises ("GIAC"), a small- to medium-sized growing business, is the largest supplier of Fortune Cookie sayings in the world. Over the last few years, however, GIAC has also felt increased competition from the rise of open source development of sayings (http://www.fortunecookiemessage.com/) as well as Wonton Foods (http://www.wontonfood.com/products), a distributor of fortune cookies who brought saying development in-house. As a result, GIAC must now continually evaluate innovative business tactics that can help them retain a market edge.

To remain highly competitive, GIAC maintains almost absolute secrecy around its ‘secret sauce’ for transforming a fortune into a GIAC fortune. We estimate that over 80% of all GIAC information carries a restricted or higher classification. Protected assets include both data, such as the fortune saying database, and closely-held business processes and workflows as well as personal information on the highly skilled staff and creative authors of the sayings.

The CIO, startled by the number of outbound connections revealed by the endpoint firewall – Little Snitch – on his laptop, convened a tiger team led by the authors of this report. Based on further discussions with the CIO, his staff, and various business owners, we formalized the three key objectives of this thirty-day study as well as established its approved scope.

- **Objective One:** Increase the security of ‘known’ employee endpoints, which for this effort will be limited to the corporate MacBooks issued to each employee.

- **Objective Two:** Increase safety of employee and contractor endpoint devices. To date, GIAC has developed policies around mobile device management (MDM) but has spent a little time in evaluating the secure use of the web browsers routinely utilized by both employees and contractors in the conduct of GIAC business. We focused our effort on remediating the increasingly adverse effect browsers might have on both GIAC and its workforce.
Objective Three: Guard against loss of GIAC competitive edge due to leaked information from endpoints. We focused on approach on the RESTful web services interface used by the contractors, both fortune authors, and fortune translators, after determining that these workflows currently provided the greatest risk to GIAC regarding the leakage of sensitive data.

This report summarizes our approach, our results, and our recommendations about these three objectives. We conducted a situational assessment, used that as the basis for a risk assessment to confirm our proposed approach. We then researched and analyzed each objective according to the accepted scope. We then prepared a final set of recommendations and next steps. Details of our research and analysis are contained in the lab report, referenced as an appendix to this report, but delivered as a separate document.

3. Situation Assessment

GIAC Enterprises is a small to medium sized growing business with a workforce of 1,000 employees, 200 people of which are in central business and IT. They depend on a large number of individual 1099 contractors, approximately 200, that submit fortune cookie sayings via a remote application. They also use contractors for fortune translation services and some limited quality assurance (QA) at the discretion of the internal GIAC QA staff.

3.1. Data Flow Analysis

Evaluation of data leakage and how to thwart possible loss should start with an understanding of how sensitive data flows through an organization (Filkins & Radcliff, 2008).

3.1.1. Employee Work/Data Flows

GIAC employees follow standards business workflows, commensurate with their roles as outlined in Table 1, and supported by well-documented baselines as to how information moves throughout the enterprise from creation to destruction.
Table 1: GIAC Enterprises Workforce

<table>
<thead>
<tr>
<th>Employees</th>
<th>Contractors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executives</td>
<td>Contractors:</td>
</tr>
<tr>
<td>Finance and HR</td>
<td>• Fortune authors</td>
</tr>
<tr>
<td>Sales and customer service</td>
<td>• Fortune translators</td>
</tr>
<tr>
<td>Research and Development (R&amp;D) and QA IT:</td>
<td>Vendors:</td>
</tr>
<tr>
<td>• Helpdesk (supporting contractors and employees)</td>
<td>• GIAC Systems (e.g., CRM, SharePoint)</td>
</tr>
<tr>
<td>• Admin servers</td>
<td>• Incident response</td>
</tr>
<tr>
<td>• Network admin</td>
<td>• Legal (outside counsel, international law)</td>
</tr>
</tbody>
</table>

There is, however, some uncertainty as to the exact nature of the workflows that involve employees in R&D and QA interacting with the 1099 contractors (i.e., the fortune authors and translators) that need better clarification.

3.1.2. Contractor/Vendor Data Flows

Table 2 provides further details on the contractor categories and roles. Sizing of the 1099 contractor workforce is dependent on the current workload, taking into account yearly fluctuation with peaks at the Chinese New Year (February), the spring solstice (March) and winter solstice (December). (Note: Section 3 of the Lab Notebook contains detailed workload information.)

Table 2: GIAC Contractor Categories/Roles

<table>
<thead>
<tr>
<th>Title</th>
<th>Role/Responsibilities</th>
<th>Sizing</th>
<th>Access to GIAC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fortune Authors</td>
<td>Develop fortunes for GIAC</td>
<td>Approximately 150 independent authors</td>
<td>Submit cookies via Fortune Web Service app, access web service through GIAC VPN</td>
</tr>
<tr>
<td>Fortune Translators</td>
<td>Provide initial QA and translation services for newly submitted fortunes</td>
<td>30 – 40 total Number established by California’s 13 threshold languages plus backup and idiomatic support</td>
<td>Review fortunes and submit translations, original and updates, through Fortune Web Service app, access web service through GIAC VPN</td>
</tr>
<tr>
<td>Title</td>
<td>Role/Responsibilities</td>
<td>Sizing</td>
<td>Access to GIAC</td>
</tr>
<tr>
<td>-------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>updates for idioms, new terms, etc. – as requested by GIAC internal QA</td>
<td>for Canada and Mexico plus backup. (Note: California is region for greatest fortune sales.)</td>
<td></td>
</tr>
</tbody>
</table>
| Vendors | Provide additional support for IT systems and additional services                    | No more than 20 that encompass remote vendor system support and additional services for GIAC business | Access backend GIAC systems through highly monitored gateway (Extranet/Office 365)  
Highly-trusted must pass stringent background checks as touch internal production systems.  
Limited risk, short term contracts, only on “need to have” or “need to know” basis |

Figure 1 shows the typical data/information flows associated with contractors.
3.2. Current Infrastructure

A recent procurement for GIAC Enterprise that involved the acquisition of a SIEM solution provided the following high-level architecture diagram (Robinson, Fletcher, & Whitteker, 2016).
Reviewing Figure 2 together with Table 2, we note that many of the contractor workflows are well monitored:

1. All contractors communicate with GIAC Contracts and Finance through email services supported by the GIAC Exchange services. All mail passes through a secure email gateway that examines both the message and the attachments for malicious content, sandboxing what is needed, and applying robust data leak protection practices based on the content.

2. All contractors are paid through electronic funds transfer (EFT); transfers are securely handled through a third party.

3. Trusted support vendors access backend services and systems mainly through the GIAC VPN. These vendors are considered trusted extensions of the GIAC workforce and are subject to stringent surveillance, both regarding data flows and the fact that their mobile endpoints are being monitored by the MDM solution that GIAC requires be installed on their systems connecting to the GIAC network.
Uncertainty, however, surrounds the activities of the 1099 contractors. Fortune Authors merely submit fortunes but they access the Fortune Web Service via the corporate VPN, and they do have edit capabilities on the site.

GIAC Fortune Translators both translate and provide some limited QA of fortunes. Some also author sayings. They also access the Fortune Web Service via the corporate VPN, and they have edit capabilities on the site.

4. Endpoint Risk Assessment and Results

Our first objective was to evaluate the GIAC Enterprise environment to uncover possible risks related to employee and 1099 contractor endpoints. The situation assessment we had just performed helped us to understand those key elements of the GIAC business – its mission statement, market position, information governance, workflows, and roles – to help establish the basis for endpoint risk assessment and prioritize the identified risks. Our findings established our proposed emphasis for further study and evaluation.

Figure 3 presents a graphical overview of the model upon which we based our risk assessment of endpoints within the established scope.
Table 3 presents the results of this evaluation, along with a qualitative ranking of the level of risk involved.

Table 3: Results of GIAC Endpoint Risk Assessment

<table>
<thead>
<tr>
<th>Use Case/Risk</th>
<th>Description</th>
<th>Remediation Plans</th>
</tr>
</thead>
</table>
| Insider threat                | Employee/contractor send information outside of GIAC endpoint protections (i.e., print or FAX intellectual property) | Admin: Establish business agreements with the main contractors/acceptable use terms with employees  
| (Low to Medium Risk)          |                                                                           | Limit access to sensitive information based on “need to know” – specifically 1099 contractors |

Figure 3: Endpoint Risk Model for Employees and Contractors

Access to the GIAC Web Service from outside a known endpoint – could be directly by malicious actor.
<table>
<thead>
<tr>
<th>Use Case/Risk</th>
<th>Description</th>
<th>Remediation Plans</th>
</tr>
</thead>
</table>
| **Known endpoint – trusted vendor** | **(Low to Medium Risk)** Vendor endpoint contains sensitive information/credentials and is compromised | Admin: Time-limited engagements  
Technical: Introduce security shim (MDM) sane as above to allow GIAC to monitor configuration, audit use |
| **Known endpoint – employee**     | **(Medium to High Risk)** Endpoint is either not configured, misconfigured, or compromised/infected and sends unauthorized information outside of firewall | Admin: Business agreements and acceptable use of monitoring  
Technical: Establish endpoint monitoring on individual endpoints (employee configured by IT, trusted vendors must accept as policy/terms of contract)  
Note: Vendors are highly monitored, but employee endpoint monitoring has been somewhat neglected. |
| **Attack on Fortune Web Services** | **(High Risk)** Endpoint presents opportunity for outside attack  
1099 Contractors are not closely monitored, BYOD | Technical: Reduce attack surface opportunities for fortune authors/translators |

Based on these outcomes, we further refined our approach to meet the study objectives. Originally, we had anticipated that we would be implementing strictly technical controls, supported to some extent by administrative policy.

After our assessment, we realized that we might need to propose changes to current business processes to achieve the objectives of the study. For example, we have proposed reducing the potential attack surface presented by the web services from both a technical (i.e., the use of Azure cloud services to replace on-prem hosting in the DMZ) and an administrative perspective (i.e., establish a “one way fortune author policy” where 1099 contractors that write the fortunes never exactly know what has been accepted as a GIAC fortune).
5. Security of Endpoints -- Employee Endpoint Analysis

The first study objective was to increase the security of ‘known’ employee endpoints, which for this effort was limited to the corporate MacBook’s issued to each employee. We developed a strategy to evaluate the MacBooks used in the GIAC Enterprise environment to uncover possible risks related to employee endpoints, including the establishment of unauthorized outbound connections.

Our approach was to determine what information is sent by the operating system (OS) and installed third party applications on the provided endpoint, accomplishing this through a combination of lab testing with research to understand:

- Risks associated with data transmitted from devices
- Classification of data being sent from devices (e.g. PII, location)
- Means to minimize the data leakage through centralized and local configuration or control

Our findings revealed the following:

- The OS sends minimal information to external parties, although some unique identifiers were discovered.
- Using third party testing on installed apps and extrapolating similarities to OS X installations, third parties receive large amounts of data directly attributable to the user. There are both localized and centralized configurations possible to control directly these exposures. Other identification methods were found during our work (e.g. geolocation) with ways to mitigate the risks identified.
5.1. **Endpoint Testing**

For company provided MacBook devices, testing was performed to determine what information is sent automatically by connections initiated from the system. To conduct this testing, a MacBook Air laptop was directly connected to a stand-alone network segment, and all information to/from this device was sent through a proxy device that attaches to the Internet. This configuration permitted all traffic to be captured and stored for analysis.

This proxy device was the default gateway for the MacBook, but to provide further analysis options, mitmproxy software installed on it. This software permitted all HTTP and HTTPS connections to be analyzed in detail and removed any problems with session encryption, as the information was decrypted when being analyzed. However, this configuration did not permit any encrypted payloads to be decoded if they were captured. This simple setup is shown in Figure 4.

![Figure 4: MacBook Network Testing Setup](image)

For the testing, the proxy system was setup and was the DHCP server to the network under test. Once this system was confirmed active, the MacBook was turned on, and any communications from the MacBook that reached the proxy computer were
captured and analyzed. This system was left enabled for one hour to ensure that any possible software that may communicate had sufficient time to do so. What would not be captured are any applications that did not run within that timeframe or applications that do not communicate on a regular basis (e.g. location tracking software).

With this testing, 59 connections were recorded leaving the MacBook system to various destinations. Of these links, only one sent further information to the target system beyond a user agent string. This information is shown in Figure 5.

![Network Traffic Example]

**Figure 5: Data connection with extra information**

Two links that were recorded provided details within the URL requested. These were relating to the iTunes store and sent a particular GUID, or Globally Unique Identifier. These are used accurately and uniquely to identify a particular computer or user on various websites.
5.2. Third Party Apps

While the majority of default applications do not offer or provide much tracking of the end system to outside parties, third party apps are entirely different. Numerous applications send Personally Identifiable Information (PII) and location information to outside locations, often done without user knowledge.

In the paper by Jinyan Zang, Krysta Dummit et al. titled Who Knows What About Me? A Survey of Behind the Scenes Personal Data Sharing to Third Parties by Mobile Apps, 110 apps were tested, 55 for the Android-based operating system and 55 for iOS (which is very similar to the OS X operation system). These 55 were chosen by selecting the top 5 most popular apps in the following iOS app store categories: Business, Games, Health & Fitness, Lifestyle, Medical, Photo & Video and Navigation. An additional five apps were chosen from each of the Health & Fitness, Navigation, and Social categories, due to their likelihood to have sensitive information (Jinyan Zang, 2015).

The results of this work are broken down in many ways, but the paper identifies that one app sent PII data to 17 different third party addresses, sent 15 different sites behavioral data and 17 sites location data (Jinyan Zang, 2015). While this is the extreme of iOS apps, it is not alone, as the average number of third-party domains information was sent to is 2.6. Andriod is no different, however for this work, we will focus solely on the iOS aspects.

Other reports have shown that third party apps download and send personal data to outside sources. In an online article by Dan Goodin, it was reported that SourceDNA found 256 apps found on the Apple store sent personal data to outside locations (Goodin, 2015). From their report, SourceDNA indicated that there were four major classes of information that was being collected within the apps tested. They were:

1) Apps installed on the device

2) Platform serial numbers
3) Hardware devices installed and associated serial numbers

4) Email address associated with Apple ID

The good news from the Goodin report is that shortly after it was posted online, Apple quickly responded and removed the offending apps in question and stated that the third party Software Development Kit being used to collect the data was using custom interface points into the devices and was against Apple’s policies.

But what do these reports and information mean for GIAC Enterprises? While it does not provide a definitive answer to what third party apps pose a problem, it does provide insight into the information that is being requested by third party apps that are similar to those available for the corporate MacBooks. Given the similarities between the iOS and OS X operating systems, the authors would argue that if an app were available on both platforms, it would be attempting to do similar activities on both platforms. As well, given the vast number of categories that the Jinyan Zang et al. report covered, from business apps to travel to fitness, the possibility of some of these apps being installed on a GIAC Enterprises laptop is high.

5.3. Other Means of Tracking Computers

Other means are used to monitor user and their computers. As previously mentioned in the Macbook connection testing section, user agent strings were sent from the system under test to the outside connections. These various pieces of information that commonly identify software installed on the computer connecting to a website were meant to be used to provide compatibility to websites. If a user was a connecting with a mobile device, make the web pages accessible to read on a small screen. If a user connected to a site and has an older version of Firefox installed, the website can know that certain features available cannot be viewed in that browser, and send the user the simpler website.
The potential impact for GIAC Enterprises is that this information can also be used to identify a computer uniquely. The more small pieces of information you have about something, the more likely it is that you can say with certainty that it is unique. For example, if you knew that a computer has Internet Explorer version 9 installed on it, that doesn’t tell you too much, as there are a lot of system with that version of IE installed (2.28% of all browsers in April 2016) (NetMarketShare, 2016). Now if you know that the computer also has Adobe Flash, Version 21.0.0.242 installed, this narrows down the number of systems that meet this criterion. If you were to add in Silverlight 5 Build 5.1.20913.0, Shockwave Version 12.2.4.194 and know that it is running in Windows 7 Service Pack 1, there is a lot more information known about the system, and more likely that this can be attributed to a smaller number of computers than the original. If you keep adding small pieces of information like this, eventually you will end up with only a limited number of computers that match this setup. (Note: This refers to browser fingerprinting, discussed in more detail in the Lab Report, attached as an appendix to this document.)

An additional means of tracking computers is through geolocation. Geolocation uses the IP address of the system in question, which is part of the IP packet that is sent from every computer. Companies have made available for free online, as well as for paid subscription offerings, the ability to query their databases to determine where an IP address is coming from. An example of one of these companies, EurekAPI, and the information they provide is shown in Figure 6.
5.4. Recommendations

For employee endpoints, there are numerous recommendations to minimize the data leaving the system involuntarily. These solutions are diverse and can work in conjunction with each other, aiding in a phased implementation approach later.
Information from the user endpoint can be configured and controlled to minimize information leakage. Tools are available, for example, to reconfigure the user agent strings within various web browsers. An example of this change within Safari is shown in Figure 7, but similar options are possible within Firefox, Internet Explorer, and Chrome, to name but a few. These setting changes are possible either directly within the application or through third party plugins. By modifying the settings on the local device, it will assist with minimizing the exposure whenever the device is connected to a network outside of work (e.g. home).

Figure 7: Safari user agent string menu
Central control of the user agent information is possible through proxy servers. These devices, such as McAfee and Websense, permit changes to the information that devices sent to the outside. Installing and configuring a proxy server to minimize and standardize the information being sent from the organization is a second step that is recommended.

Another recommendation is to evaluate if geolocation obfuscation is needed for GIAC Enterprises. Based on the current information it is not, but not all details were available for this report. A risk analysis of the business drivers behind this functionality should occur sooner than later to determine if needed.

Finally, user awareness and training is required, both to understand the new tools that may be deployed, but also to provide the background on why these new techniques and processes and being put in place. Many changes can be performed locally on the system, and the end users can change/modify these setting. For true buy-in from the employees, they need to understand the risks associated with the various actions and how this affects their safety and security. Then and only then will full buy-in happen from the employee base for these new processes and technologies.

6. Safety of Endpoints – Considers the Browser

The second study objective was to increase the safety of employee and contractor endpoint devices. GIAC staff and contractors share a common safety element – the use of the browser on their endpoint. GIAC has developed policies around mobile device management (MDM) but has spent relatively little time in evaluating the secure use of the web browsers routinely utilized by both employees and contractors in the conduct of GIAC business.

Using research resources and available tools, we explored issues around safe browsing, seeking to improve browser security with a goal of protecting both the GIAC
workforce and the enterprise GIAC from costly cybercrime, such as malicious online advertising.

A March 2016 “Malvertising” incident of which affected numerous mainstream websites, with victims that included The New York Times, the BBC, MSN, and AOL. The code tries to avoid a long list of security products and tools to remain undetected. If the code does not find any of these programs, it appends an iframe to the body of the HTML that leads to Angler EK [exploit kit] landing page. Upon successful exploitation, Angler infects the poor victim with both the Bedep Trojan and the TeslaCrypt ransomware. (Chen, 2016)

We investigated some of the biggest problems that plague browsers. Browser vulnerabilities encompass the actual software, its configuration, the management of that configuration by the end user, and the interaction of that configured browser with the given site it is accessing. We found, however, that most problems distil down to three core areas, details of which can be found in the attached Lab Report:

- Browser Configuration Consideration: What browser should be used? How should it be configured? What are the plugins that might support security?
- User Browser Management: How often should a user clear the cache?
- Tracking Privacy: What should users know about privacy tracking, both for personal safety and for the safety of the enterprise?

6.1. Analysis Summary and Decisions

A review of the threats to endpoint browser security resulted in a set of best practices along with recommended policy (either paper or system based) and procedures as presented in Table 4. We also indicate whether, in general, the policy and procedure applies to the employee, the contractor, or both. (Note: Some of these echo recommendations provided in the previous section.)
The list of recommended policies and procedures should be continually reviewed and updated as new browsers and related automation reach the market as well as new exploits come to light.

**Table 4: Best Practices for Web Endpoints**

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Recommended Policy/Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determine GIAC browser and minimum secure configuration guidelines</td>
<td>Establish a list of allowed browsers that, as part of MacBook image, are permitted. Establish white list/black list so unauthorized browsers cannot be installed or will be identified and removed if installed. (EMPLOYEE) Provide list of recommended browsers for contractors to access Fortune Web Service, including clear instructions for configuration (CONTRACTOR)</td>
</tr>
<tr>
<td>Keep browser and underlying operating system updated</td>
<td>Incorporate web browser updates in patch management procedures, audit configuration with tools such as Qualys. (EMPLOYEE) Consider having contractors present evidence of current browser configuration with a tool such as Qualys, requiring documentation of test results at various periods (i.e., initial contract, contract renewal) (CONTRACTOR)</td>
</tr>
</tbody>
</table>
| Identify and implement additional browser features and plugins for protection | Activate the following functions:  
  - Protection against malicious sites such as:  
    o Internet Explorer: SmartScreen Filter  
    o Firefox: Displays a red warning message and blocks access to malicious websites  
    o Chrome: Sandboxing, auto updates (EMPLOYEE)  
  - Domain checking against deceptive internet sites (such as Domain Highlighting in IE) (EMPLOYEE) |
### Best Practice

#### Recommended Policy/Procedures

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Recommended Policy/Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable endpoint firewall (EMPLOYEE)</td>
<td></td>
</tr>
<tr>
<td>Configure for the proper use of TLS (EMPLOYEE)</td>
<td></td>
</tr>
<tr>
<td>Enable browser protections for phishing and malware (EMPLOYEE)</td>
<td></td>
</tr>
<tr>
<td>Establish user browser management guidelines (e.g., cookie management, cache, and local storage management)</td>
<td>Provide training and awareness, preconfigure browsers for proper action (such as knowing how and when to clear the browser cache or local storage) (EMPLOYEE)</td>
</tr>
</tbody>
</table>
| Identify and implement tools for private browsing | Evaluate and activate (or provide instructions to users on how to activate) those tool options for private browsing:  
- Pages visited will not be recorded in the history or address bar  
- Cookies will be deleted at the end of the session  
- The cache that stores temporary Internet files will be emptied at the end of the session.  
- Forms, search bars, and text boxes will not save the data you have entered, including passwords.  
- Downloads listed in your download window or folder will be deleted, although the download itself will remain on your computer. (GCF Free Learning, 2016) (BOTH CONTRACTOR AND EMPLOYEE) |
| Provide user education and awareness on secure browsing | Make sure individuals have the understanding and ability to:  
- Identify (e.g., green bar when EV certificate has been recognized) and verify a secure site (i.e., presence of https and a locked icon that provides information) and what actions to take if there is an |
<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Recommended Policy/Procedures</th>
</tr>
</thead>
</table>
| Identify an issue                                 | • Identify a certificate error and what steps to take if there is an issue or error  
• Comply with safe download procedures, such as saving first then running or concerns with freeware, shareware or bloatware  
• Avoid clicking on suspicious links, such as ads presented by known, mainstream sites (BOTH EMPLOYEE AND CONTRACTOR)                                                                                                                                                                                   |
| Provide user education and awareness on private browsing | Ensure that users understand the limitations of privacy browsing and the supporting tools. For example, private browsing does not make a user anonymous on the Web. Websites can still track your visit and activity through the IP address  
Ensure that users comprehend how browsing activity can be tracked and used for and against an individual such as  
• A website places a cookie on your computer to remember certain data so it may run smoother when you return to the site.  
• Web sites like Amazon, eBay, and Netflix collect data about your preferences so they can make suggestions to you for products or movies they think you might like.  
• Google tracks and analyzes activity to provide statistical information to companies for marketing or advertising purposes or to examine the effectiveness of a website. |
### Best Practice

<table>
<thead>
<tr>
<th>Best Practice</th>
<th>Recommended Policy/Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Some governments may collect data about online activity in case it is needed for criminal investigations or national security purposes.</td>
</tr>
<tr>
<td></td>
<td>• Sometimes by downloading a program or signing up for a website, you agree to allow the program or site to collect data that may be provided to third parties for advertising.</td>
</tr>
<tr>
<td></td>
<td>• If you share a computer, other people can spy on your activity by reviewing your browsing history. (GCF Free Learning, 2016)</td>
</tr>
<tr>
<td></td>
<td>• Most malware or spyware is used to track and obtain sensitive information like credit card numbers and bank account passwords that can be utilized for identity theft crimes (BOTH EMPLOYEE AND CONTRACTOR)</td>
</tr>
</tbody>
</table>

### 7. Web Service Endpoint – Fortune Web Services

The third study objective was to guard against loss of GIAC competitive edge due to leaked information from endpoints. Our focus here is to reduce the risk posed by the current architecture by providing a secure cloud-based application for contractors (fortune authors and translators) to provide fortune content while protecting corporate production assets.

We evaluated the development and deployment of a sample application on Azure to understand the process, assess development time and options, as well as to investigate the ability to monitor a cloud-based implementation and identify key security aspects for AppDev.
We used well-defined Microsoft application development patterns to prototype a cloud-based web application that would totally remove 1099 contractor access to any part of the “on-prem” GIAC Corporate network while providing improved tracking and analytics for all user activity. Also, we felt that a cloud-based solution could provide 24 by 7 availability in a global market while potentially improving/lowering support costs associated with service desk request such as password resets.

We were pleasantly surprised at the results. Our prototype application took less than twelve hours to design and implement. Microsoft’s Application Insights, as well as the standard Azure security monitoring, provides a robust and dynamic capability for visualizing activities and security issues.

In the long term, a cloud-based Azure implementation can help contain or even reduce support costs. Further analysis is needed, especially a cost-benefit analysis based on formal requirements (including AppSec) and sizing estimates that can provide an accurate comparison of estimated Azure costs with what GIAC is spending today.

### 7.1. Design Considerations—As-Is Versus To Be

Figure 8 shows the “as is” process for submitting and translating fortune sayings.
The Extranet DMZ at the GIAC Data Center hosts the Web Service endpoint. While network protections are in place, there is always the chance that an exploit could compromise the systems in the Extranet DMZ and pivot from there to infect the GIAC production network in a moment of weakness, such as during a patching or update cycle.

The current approach places an unnecessary burden on GIAC IT resources. All 1099 contractors, both fortune authors, and translators must have correctly named accounts for GIAC VPN account as well as Web Service site access. Service desk staff, particularly in those peak development times during the year (the Chinese New Year, the spring solstice, and winter solstice) are often overloaded by password reset request from 1099 contractors, especially fortune authors. Contractors that use their mobile devices (BYOD) for submitting sayings must agree to abide by GIAC MDM policies (such as remote wipe). This has proved a deterrent to engaging fortune authors as well as (again) placing an additional burden on GIAC IT staff to manage.

The design of the Web Service site also exposes 1099 contractors unnecessarily to sensitive information. Fortune authors know which sayings have been accepted into the GIAC production dataset. There is also no separation of role between author and translator, allowing even greater exposure to GIAC intellectual property and especially critical because the author and translator role cannot be easily monitored as separate roles.

Based on the “as is”, we can sum up the requirements that the “to be” process must meet as 1) be more secure than the current process (i.e., separate from the GIAC corporate network), 2) reduce the burden on IT, and 3) provide better control over sensitive data with better separation of duties (roles) and improved monitoring.

Figure 9 details our proposed “to be” process that will utilize the Azure cloud to host the GIAC Web Service.
This solution meets our basic requirements. The entire process is in the cloud, separated from the GIAC production network at all times, except when GIAC IT initiates a data sync between the on-site SQL development or production databases and the Azure SQL staging tables. While infection of the GIAC internal network could still occur, this approach reduces that risk.

The proposed Web App allows 1099 contractors to manage their credentials, reducing the existing burden on GIAC IT. Contractors can use their OAuth credentials or turn to self-service password reset, through either email configuration or SMS. Multifactor authentication is available. Eventually, GIAC may decide to authenticate translators through Active Directory services, integrating Azure AD with the existing internal GIAC Windows AD.

The newly designed Web App provides better control over sensitive data. The roles of Author and Translator have been re-defined: an author can only edit up to the
time he/she submits a saying; a translator may edit on an entire dataset until the dataset is submitted.

We propose that GIAC should also back the new Web Services platform up with an administrative policy and business procedures that further eliminate a fortune author’s knowledge of IP. The “one-way fortune author policy” would support a payment scheme that aggregates payment on volume submitted and number accepted without providing any additional detail. Authors know the number they have submitted, and the percentage of that has been accepted, but they are not aware of the actual sayings that have been accepted. Furthermore, an author cannot be – at least concurrently – a translator, so they are not exposed in any way to the sayings that have been accepted.

Lastly, the Azure service provides in-depth monitoring tools, both through the native platform and Application Insights, which allows monitoring of a wide variety of parameters including the ability to correlate actions taken by the Web Service (PUT, GET) with database activity

7.2. Approach

The prototype required the use of Visual Studio 2015 first to develop and test the app locally and an Azure subscription (a free one comes with an MSDN subscription) to deploy to the cloud.

This application is based on ASP.NET MVC (Model View Controller), a web application framework developed by Microsoft from the model–view–controller (MVC) pattern, which is open source. This allows software developers to build a web application as a composition of three roles: Model, View, and Controller. The MVC model defines web applications with three logic layers:

- Model (business layer) – the state of a particular aspect of the application
- View (display layer) -- accepts necessary information from the controller and renders a user interface to display that information
• Controller (input control) -- handles interactions and updates the model to reflect a change in state of the application, and then passes information to the view. (Wikipedia, 2016b)

Details of the development are contained in the Lab Notes attached to this document as an Appendix. The entire process of standing up the prototype took approximately twelve hours. Additional time was needed to configure Visual Studio and enable monitoring in the Azure environment.

7.3. Observations from Prototype

Ease of deployment and depth of monitoring make this an attractive solution for fortune saying submittal and translation by 1099 contractors. To ensure the Web Service endpoint is secure, additional work is still needed.

GIAC must address security considerations throughout the design and deployment of the “to be” process. The security checklist should address:

• Secure management of credentials needed by the Web App. This includes username and passwords for support services like SendGrid (supports password reset by email) or the SMS provider (multi-factor authentication), certificates, and keys.

• Security testing, addressing first the straightforward functional testing and then using risk analysis and threat modeling to establish possible adverse scenarios and related test requirements.

• Verifying that the inter-process communications between the Web App and other Azure services are secure as well as those external channels, such as the SQL database sync from Azure to GIAC.

• Use of a Web Application Firewall to guard against web-based vulnerabilities that include the OWASP Top 10. ModSecurity can be configured to work with
an Azure-deployed web app or providers like F5 and Barracuda have services available through the Azure Market Place.

- Periodic vulnerability scanning, using either the “one-click” service available in Azure from Tinfoil Security or through a third party, after obtaining approval through the established Azure penetration testing approval process.

The depth of information available in the analytics and analysis options offered with Azure for support and review will provide a welcome challenge for GIAC IT. Detailed audit information is exported to the Microsoft on-line PowerBI tool that is linked to the database through the Azure subscription. The following images show snapshots from the resulting dashboard that can be used to audit and track SQL server activity on Azure.

Figure 10 shows the overall status of the Web App by resource type. Note that activity on the Application Insights (Insights), The Web, database (SQL), and SendGrid are among the activities that can be monitored.
Figure 10: Azure Status Dashboard

Azure events can be imported in Microsoft’s on-line PowerBI. The interface, shown in Figure 11, allows for customization of the reports and visualizations.
8. Summary and Recommendations

This work started with a simple request from the CIO, a request to understand what information was being sent from the endpoints within the organization without user knowledge and what risk this posed to the organization and its workforce. As it turns out, a simple request with a complex set of answers. We reiterate the study objectives here for reference:

- **Objective One:** Increase the security of ‘known’ employee endpoints, which was limited to MacBooks that are issued to each employee.

- **Objective Two:** Increase safety of employee and contractor endpoint devices. The effort was focused on remediating the increasingly adverse effect browsers might have on both GIAC Enterprises and its workforce.
Objective Three: Guard against loss of GIAC competitive edge due to leaked information from endpoints. We focused on approach on the RESTful web services interface used by the contractors for both fortune authoring and fortune translating.

Sections 5 through 7 explored these objectives in detail, providing recommendations and solutions for each, but GIAC will need all these suggestions to work hand in hand to increase the overall security posture of the enterprise.

GIAC must first acknowledge that data leakage at some level will always occur; the enterprise will never completely prevent some level of exfiltration. The very architecture and core of how the Internet was setup, configured, and functions ensures that some information will always dribble out from the endpoints connected to it. However, the volume of information and how it is shared is possible to control. This is the assumption we are basing the following recommendations upon.

**Recommendation 1:** GIAC employee endpoints need stronger controls to minimize the data provided to third parties.

The approach to meeting this recommendation has several elements; each should be evaluated by GIAC for how best to implement. First, employee devices need to have enabled the ability to change user agent strings. The IT department should manage this capacity centrally. A means to push the changes out to the end user devices must be found that removes reliance on the end user to perform any changes.

Next, a means must be found to check settings in use on devices. The capability is available in most modern browsers, such as Firefox, Safari, and Internet Explorer, to alter these settings. IT should determine the minimal configuration that permits users to perform their duties while minimizing and standardizing the information shared outside of the organization. These changes will assist with the devices when they are directly connected to the Internet, such as when an employee takes the device home.
A second central solution should be configured and deployed within the corporate setting. We recommend a modern proxy server that terminates all internal requests, and initiates new connections to the outside be installed. This is key to the success of Recommendation #1. The device must permit the manipulation of the user agent strings that are sent publicly.

**Recommendation #2**: GIAC should deploy a new cloud-based architecture for submittal and translation of fortune saying to reduce the security concerns around unmanaged contractor endpoints.

Currently, 1099 contractors can access GIAC enterprise systems, albeit in the Extranet DMZ. The security and safety of the contractor endpoints are a concern, particularly since the business has no management or control over these endpoint devices since they belong by independent contractors. GIAC needs to identify a solution that removes the need to control the endpoints.

A move to RESTful, Azure-based cloud services can minimize the access to the corporate network, and increase the security surrounding GIAC’s sensitive data. Our proposed solution will also improve monitoring ability of GIAC Enterprises.

**Recommendation #3**: GIAC should develop a policy and process for the approval and management of apps authorized for installation on corporate devices.

We make this recommendation because of the extensive amount of data that third party apps send out from the devices upon which they are installed. GIAC needs to test these apps to determine if they send information out from the system and permit the organization to test properly and implement any changes required to minimize this leakage.

**Recommendation #4**: GIAC should evaluate the corporate need for IP address masking and obfuscation.
Today’s networks require the sender’s IP address be shared with the destination system to enable end-to-end communications. We recommend that GIAC Enterprises evaluate the corporate need for IP address masking and obfuscation. Based on available knowledge, we feel that implementation does not need to be immediate, but we recommend that GIAC evaluates this recommendation reasonably soon.

**Recommendation #5:** GIAC should create and provide user training on the protection of sensitive information.

We recommend that user training is created and given to the GIAC workforce so that a real understanding of the risk that the leakage of sensitive information presents to the enterprise and its workforce. Users help ensure the GIAC systems remain guarded against data leakage. Without proper understanding, an end user may not fully engage in the protection processes. An awareness/education program is necessary to help the users understand concerns and risks, to both the organization and themselves, and how why these measures are needed.
9. References


## Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Course Name</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Amsterdam August 2020 Part 1</td>
<td>Amsterdam, NL</td>
<td>Aug 03, 2020 - Aug 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS FOR508 Canberra August 2020</td>
<td>Canberra, AU</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam August 2020 Part 2</td>
<td>Amsterdam, NL</td>
<td>Aug 17, 2020 - Aug 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Virginia Beach 2020</td>
<td>Virginia Beach, VAUS</td>
<td>Aug 31, 2020 - Sep 05, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Philippines 2020</td>
<td>Manila, PH</td>
<td>Sep 07, 2020 - Sep 19, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London September 2020</td>
<td>London, GB</td>
<td>Sep 07, 2020 - Sep 12, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Baltimore Fall 2020</td>
<td>Baltimore, MDUS</td>
<td>Sep 08, 2020 - Sep 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Threat Hunting &amp; Incident Response Summit &amp; Training 2020</td>
<td>New Orleans, LAUS</td>
<td>Sep 10, 2020 - Sep 17, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online-US</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only-US</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>