Dolvin Consulting, Inc

Incredible and True Case Studies

A whitepaper provided by: InterGuard

Three Case Studies to Amaze

Best Use of Time

Our first story comes to us from one of our clients with a company with 53 employees. The organization had grown from a small group of 10 to the larger group of 53 over the course of 14 months. As they grew they realized that they needed to implement IT security measures in their work environment to make sure that critical data, assets and performance measurements were in place to monitor all of the new employees.

One of the solutions InterGuard provides is a powerful Web Monitoring and Blocking service. The software works on and off network. What's more, it is easy to use when profiling different types of online activities that should be blocked such as gambling sites, pornography sites, and streaming video or audio, which can all be big bandwidth hogs and will slow down performance for all users on the network.

The CEO was very involved in the selection process, for the InterGuard security solution and put the web blocking and monitoring services to work based on simple profile options. The goal for the CEO was to make sure that everyone was being productive. What he got was a lot more.

The day after the InterGuard services were launched he noticed one of his employees was accessing a web site that provided live video from the sets used for the television show Big Brother. Not only were they accessing the site, but the employee was on for large portions of the day. The employee was one of the company's longest tenured and it was a great surprise to the CEO. He wasn't sure if it was a mistake or maybe just an odd day so to make sure it didn't happen again he blocked that site for the company with a few clicks of the mouse using the InterGuard web portal.

Well as it turns out the next day that long tenured employee, discovering they couldn't watch the Big Brother video at their computer, went to several other employees' desktops trying to gain access. The employee quickly discovered that they couldn't access the show on any computers and actually went to the CEO to ask if something was wrong with the internet. Needless to say, the CEO had a long talk with the employee about web usage in the office and what the company expectations were for work time. The CEO subsequently learned that many employees were aware of the behavior of the long tenured employee and were annoyed but didn't know what to do and it had lowered morale in the office.

Where O Where Are Our Computers

One of our client companies, let's call them Acme Corp., has our services installed on all of their company desktops and laptops. Acme has InterGuard services for Employee Monitoring, Web Filtering and Data Loss Prevention. One of the additional services Acme uses is for laptops and is called Laptop Cop. Laptop Cop ensures that laptops can be controlled or locked down remotely if stolen or lost and has the added benefit of being able to track the laptop itself geographically, often better than GPS. Acme has 23 employees and has been a client for several years and has found the InterGuard services

cost effective with several specific examples of how the service more than covered the cost. On this occasion it had possibly the highest ROI.

Not too long ago the CEO of Acme came to the office early as he typically does. He is usually the first employee in the door each day. On this particular day the office looked a little different. During the night the office was robbed and the computers had been stolen from the desks. Desktops, monitors and laptops were all missing. The CEO immediately called the police and started going through the standard procedures. As the employees started showing up for work they learned of the crime. While everyone was trying to figure out what they could do without their computers the IT administrator got to work on his laptop that he had at home the night before.

The IT Administrator knew that the stolen laptops had Laptop Cop installed and it represented an opportunity to at least find some of the computers. He logged into his secure InterGuard web portal and activated Laptop Cop. Within a few clicks he was tracking the laptops on his computer. He shared the mapped location information with the CEO and the police and they were able to locate and recover the cache of computers and other stolen merchandise within hours of the break in.

Never Know When It Helps

We have the good fortune that many of our customers are not only clients but fans of the InterGuard solution as well. Last year one of our bigger fans/customers who is in the insurance industry (we'll call him Sam) was presenting the InterGuard solution to a larger group of insurance agency owners and unintentionally had a live presentation of the value of InterGuard services.

The focus of Sam's presentation was how to use security solutions in his business environment, and how other business owners could also benefit from employing similar tools. When Sam started reviewing the InterGuard solution he was focusing on how it was simple enough even for him to use, poking fun of himself. He accessed his InterGuard secure web portal and was reviewing live information including web site blocking, any alerts about misappropriate language or key word usage as well as monitoring email usage.

To demonstrate the software's capabilities he clicked on an employee's actions and he immediately noticed that one of his top salesmen was accessing a webmail web site. Pointing out that if he wanted to he could take a deeper dive and see what the employee was using the company owned computer and web access to communicate about. He decided to click on the example just to exhibit the security information he could access.

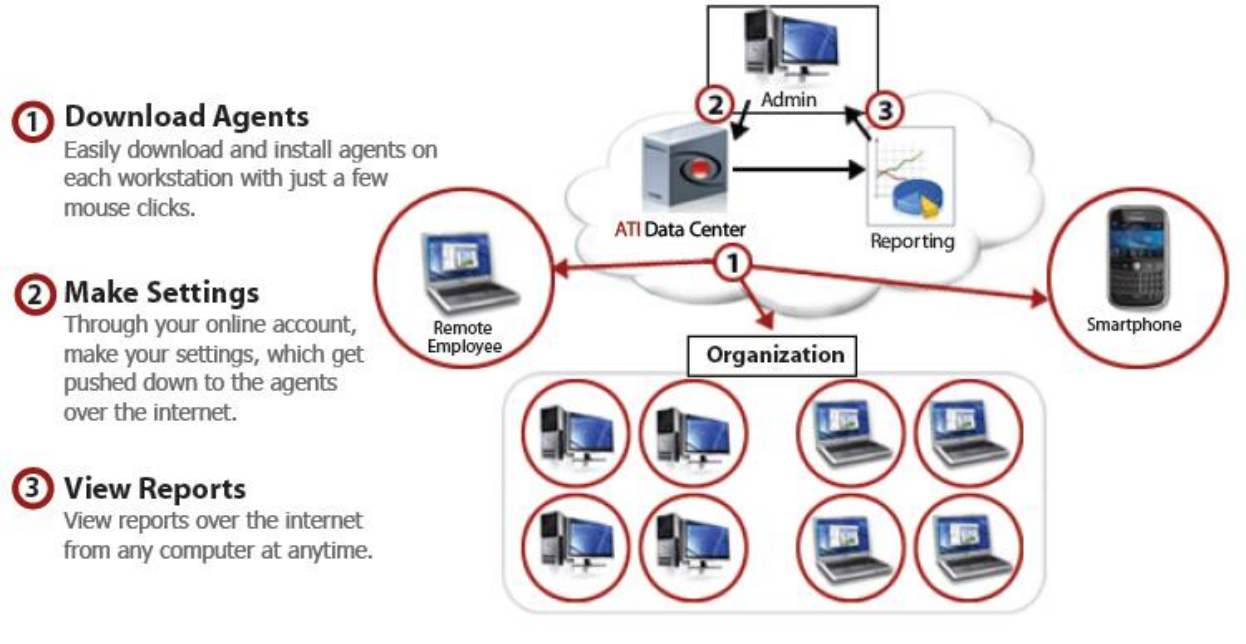
Well to his surprise, Sam discovered that the email that the salesmen had sent was an email from his salesperson to a competitor informing him that he could obtain and bring with him a file of customers and proprietary company information when he took the new job with the competitor next week. When Sam realized what the communications covered and recovered from his shock of experiencing this scheduled theft of company assets (the customer list) as well as the actions of his turncoat salesperson he recovered quickly. He made a few well-placed jokes to the audience, pointed out that there wasn't a

better example of the value of the InterGuard solution despite the fact that he hadn't intended to present a real time example. Of course Sam wrapped up quickly after leaving the podium and logged back into the InterGuard solution, clamping down all security protocols on the salesperson's computer and then quickly fired the employee via the phone.

The InterGuard Security Solution

Endpoint security has become much more necessary as network based solutions do not adequately account for off-network staff. What information security professionals need is a next generation endpoint solution that focuses on the insider that works everywhere and sees everything. No excuses or exceptions for telecommuters, travelers, and other remote employees. No security gaps missed by lack of visibility across all endpoints, PCs **and** smartphones, regardless of location.

Simple, Complete SaaS Solution



InterGuard

Deployed at the endpoint, InterGuard defends your business from all insider threats through a cloud-based delivery model. From one desktop agent and one interface, clients can access 5 technologies including Data Loss Protection, Web Filtering, Employee Monitoring, Laptop Recovery, and Smartphone Monitoring. Our solution is offered as both a complete suite or as five individual modules and is offered through the cloud so there is no hardware to buy, install or manage. Installs are fast and easy with no ongoing management required.

1. *Web Filtering*

- Monitors and filters internet use on and off the network (even on laptops).
- Blocks or limits applications like peer-to-peer and instant messaging.
- All search terms captured
- Screenshots taken whenever an alert word is typed or read on a webpage.

2. *Data Loss Prevention*

- Protect and enforce policies governing each employee's computer use, including those that never connect to a network, including laptops.
- Detect and block non-public personal information (NPPI) from leaving your network or organization , either via email (both Outlook and webmail) or USB
- Scan all PCs (including if off-network) for sensitive/confidential data
- Stop the use of removable media.
- Easy intuitive policy creation.

3. *Employee Monitoring*

- Records all PC activity including employee communications (email, webmail, and instant messaging) programs used, websites visited, search terms used and keystrokes.
- Screenshots taken whenever an alert word is typed or read on a webpage.
- Blocks or limits applications like peer to peer, webmail and instant messaging.
- Formats all data into easy-to-read reports, making it easy to find and evaluate critical security lapses.
- Ability to search all stored data based on alert words as well as sender or recipient.
- Full individualized reporting on an employee's computer activity.
- Works invisibly and undetectable at each desktop, without impacting central network computer resources.
- Ideal complement to DLP by recording all PC activity. Since DLP is rule-based, you don't know what has been missed. Allows for DLP fine-tuning and forensics in case of data-breach.
- Ideal complement to Web Filtering by recording all PC activity instead of just websites since time wasting activities on a PC extend beyond simple websurfing.

4. *Stolen/Lost Laptop Protection*

- Geo-locate all laptop locations
- Remotely retrieve/delete important files invisibly, using any internet connection.
- Monitor everything the thief does including all of the files they attempt to access, etc.
- Prevent the thief from being able to access to any desired programs (Excel, Word, etc.)
- Remotely delete files or an entire hard drive.

5. Smartphone Monitoring

- Monitor and record smartphone messages, including SMS and email
- Get notified via email when select keywords are found in messages
- Select important keywords to have them highlighted in user-interface for easy access
- Access the account from any web browser along with all other InterGuard services

Looking For Some Additional Information? Contact Us Today

CONTACT INFORMATION

- ✓ *NAME-* ***MICHAEL DECAMILLIS***
- ✓ *COMPANY-* ***DOLVIN CONSULTING, INC***
- ✓ *PHONE-* ***609-771-8141***
- ✓ *EMAIL-* ***INQUIRY@DOLVIN.COM***
- ✓ *WEBSITE-* ***WWW.DOLVIN.COM***