Business challenge

CyFIR, LLC wanted to create a forensic security application that would be more proactive in seeking out and remediating security threats than other solutions in the marketplace.

Transformation

CyFIR worked with IBM to integrate the capabilities of IBM® Resilient Incident Response Platform® (IRP), IBM BigFix® and IBM i2® Enterprise Insight Analysis technology with the CyFIR platform. The result? A comprehensive threat detection and remediation platform that can help customers drastically reduce the costs associated with a security incident.

Results

Reduced costs by up to 90 percent
per security incident investigation

Cuts time required for malware detection
from up to hundreds of days to just 15 minutes

Reduces resolution time for security incidents
from two months or more to just 1-2 days

CyFIR, LLC

Proactive security capabilities significantly cut costs

Headquartered in Ashburn, Virginia, CyFIR provides solutions for incident response, internal investigation, e-discovery and threat assessment. Formerly known as CyTech Services, which was founded in 2002, the business has approximately 35 employees.

"Ten years ago, you knew where your perimeter was—it was in your data center. Where is your perimeter now? It's out there in the cloud."

—Brian Cook, Chief Executive Officer, CyFIR, LLC

Share this

Security for when the outer defense fails

Regardless of its primary mission, today, every company is essentially an IT company. "You may be a shipping company, but really, you're an IT company that does shipping," says Ben Cotton, Founder at CyFIR. "Technology is now the competitive differentiator in all industries, so if you're not thinking in terms of protecting your IT, you should be."

It's important to protect your IT infrastructure for many reasons. Hackers could be planting malware. A competitor or disgruntled employee could try to steal intellectual property (IP). "It's not just enough to prepare to defend your infrastructure; it's critical that you prepare for when the defense fails," Cotton asserts. "From a planning standpoint, you can't count on keeping them out. You have to have a plan for when they get in."

The rise of the cloud has only made security more challenging. "Ten years ago, you knew where your perimeter was—it was in your data center," says Brian Cook, Chief Executive Officer at CyFIR. "Where is your perimeter now? It's out there in the cloud. What if you have a bring your own device policy? How do you protect your IP in that situation?"

To help businesses stay on top of all these issues, CyFIR wanted to develop a more proactive approach to threat detection and mitigation. "We weren't satisfied with just looking at things post-breach, with being reactive," says Cook.

Proactive scanning plus automated mitigation

CyFIR is working with IBM to merge the functionality of BigFix, Resilient IRP and i2 Enterprise Insight Analysis technology with the CyFIR platform. "The IBM toolset is fantastic for CyFIR," remarks Chief Product Officer John Irvine.

The CyFIR program forensically interrogates multiple endpoints simultaneously across vast networks, looking for known malware along with unknown objects. The company maintains a catalog of known malware and can easily identify objects that have been seen before. However, new vulnerabilities are constantly being developed, and identifying them is more challenging. Therefore, as the CyFIR platform queries each endpoint, it also looks for unknown entities, meaning programs or files that are neither known malware nor objects that are part of an endpoint's typical operating system, application files or patches. If the program finds an unknown entity, it acquires it, executes it and analyzes it to determine if it's malicious or benign. In the case of a new unknown entity, it could take up to 15 minutes to analyze.

CyFIR feeds the data it gathers to the Resilient Platform. The solution delivers security orchestration and automation, collecting data and then providing instant mitigation capabilities. The application also provides a digital playbook that helps automate initial triage steps when a threat is identified, freeing analysts from performing repetitive, manual tasks.

When a potential problem is detected, CyFIR uses the BigFix application to automate the necessary analytics, acquire the affected memory or hard drive, and put the affected areas into an automated workflow for issue remediation. "What BigFix does extremely well is perform individual functions on a set of systems," says Cotton. "BigFix can isolate those systems from the network, perform complete remediation and reduce the risk of malware spreading."

Through integration with the i2 software, CyFIR gathers information telemetry data from endpoints. "We can almost instantly get an overview of machines talking to each other," says Irvine. "We can feed that information into i2, along with the other data i2 pulls in, giving an analyst a tremendous overview of network activities."

Rapid remediation cuts costs

By combining the CyFIR platform with the Resilient IRP, BigFix and i2 intelligence analysis applications, CyFIR can offer its customers tremendous benefits. Because CyFIR is proactively seeking out malware, it can reduce the time to detection from hundreds of days to just 15 minutes. Plus, the company can help remediate those threats remotely, significantly reducing costs. "The benefit of remote remediation is that we can resolve the issue within 1-2 days versus 60-plus days," says Andy Ward, Chairman of the Board of Directors at CyFIR. "As a result, the disruption caused by an incident decreases dramatically. And the costs of mitigation can decrease by 75 percent or more." One of CyFIR's customers, a large financial institution, reduced costs by 90 percent per security incident investigation, which amounted to a savings of USD 450,000 annually.

CyFIR can also help customers with issues beyond traditional security, such as e-discovery as part of an HR investigation or a risk assessment prior to a merger or acquisition. "Companies that are looking at acquisitions, they integrate with the company they've acquired and find out that they have been breached," says Cook. "By scanning the network with CyFIR first, now I'm buying this company that I know has a secure network."

Solution components

- IBM® BigFix®
- IBM i2® Enterprise Insight Analysis
- IBM Resilient Incident Response Platform®

Take the next step

To learn more about the IBM solutions featured in this story, please contact your IBM representative or IBM Business Partner.

Please Recycle

20024720-USEN-00