Protecting Sensitive Intellectual Property Through Unprecedented Visibility and Access Control Across Network Connections

EXECUTIVE SUMMARY

One of the largest corporate enterprises in the world wanted to catalog all of the documents flowing through their various networks according to categorizers. Bayshore SE™ (Secure Enterprise) provided unprecedented visibility and access control, and the Bayshore SE solution mitigated rogue insider and Advanced Persistent Threats to sensitive Intellectual Property.

THE CHALLENGE

The top executives at one of the largest corporate enterprises in the world presented a unique requirement. They wanted to catalog all of the documents flowing through their various networks according to categorizers. These categorizers would provide detail on high-clearance confidentiality data, such as top-secret government and military projects, high-value customers, and so on.

They wanted to be able to identify, on the fly, which documents on the network represented confidential intellectual property or institutional knowledge. Additionally, they wanted to be able to create and deploy the categorization scheme in secrecy – without their partner solution providers or even their own IT department knowing how the scheme works. And finally, once the sensitive documents were categorized, they wanted to be able to track where they were going in the network and who was accessing them.

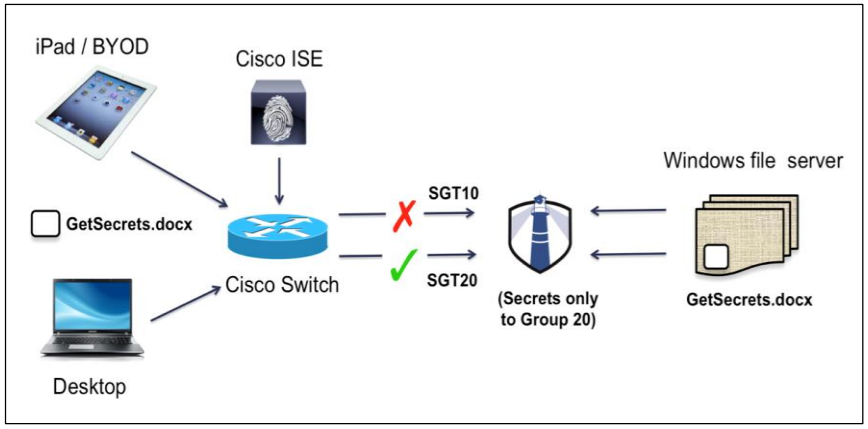
THE SOLUTION

Bayshore Networks proposed an innovative approach to protecting the executive team's corporate IP. The Bayshore proposal won in a bake-off against several market-leading solutions. By providing deep content inspection at line rate, the Bayshore SE solution mitigated rogue insider and APTs (Advanced Persistent Threats) to sensitive Intellectual Property. While traditional DLP (Data Loss Protection) solutions prevent sensitive content from crossing network

boundaries, Bayshore SE provided unprecedented visibility and access control by evaluating the content moving across network connections.

Additionally, the Bayshore solution is able to protect the sensitivity of the data internally. "We don't even know what kind of documents we're inspecting," explains Francis Cianfrocca, Bayshore Networks' CEO. "When they pulled the trigger and started using real categorizers, the Intellectual Property was only available to a select few – not even the IT guys. That's how sensitive the information is."

The Bayshore SE solution is inspecting not only documents such as PDFs, but also archives such as Zips and Tarballs. "Our ability to inspect files within files turned out to be an important differentiator," recalls Cianfrocca. "In addition, Bayshore SE also supports a broad array of protocols, not just the web traffic and file shares. We can take a look at anything moving through the network."



Deploying at network choke points such as gateways, the Bayshore SE solution establishes policies that define access privileges for documents according to their confidentiality levels.

The key differentiator for Bayshore SE is Pallaton™, an extensible policy language, which evaluates and enforces content. Pallaton's flexibility enables the Executive department to track usage patterns and to create classifications by people, by document, by traffic, or even by metadata. They can create content around any of their categorizations and then create policy around it, mitigating rogue insider threats and APTs.

Bayshore inspects data transmitted across the network as a result of access to:

- File-repository web applications
- Windows file shares
- NFS mounts
- Email attachments
- FTP sites

Pallaton rules are quickly configurable – particularly for the Executive organization, which had already created its own data content categories. Pallaton inspects Layer 7 content and makes rules-based decisions dynamically, in real-time, enabling policy evaluation to become policy enforcement.

Bayshore SE's advanced features for High-Value IP Protection provide extremely high performance, configurability tailored to the customer's categories (not signatures), and actionability enabled by enforcement of policies.

RESULTS

The executive team, which houses their sensitive IP in a specific topology, deployed Bayshore SE in a strategic gateway. This enabled access control in and out of the confidential environment. Bayshore's 10-Gbps-plus performance enables them to use Bayshore SE inside the network. Reports can be generated via Splunk or other tools.

Additionally, Bayshore SE's user-configurable rules also inspect outside content; competitive solutions offer bundles of signatures that are difficult to customize. Bayshore SE's application-layer inspection capabilities enable it to inspect every level of every document in an archive. It can extract and inspect content from multi-level archives such as Zips and Tarballs, and utilize the customers' existing YARA rules.

"A key differentiator against the competitive solutions is that we were able to allow the customer to easily ingest their own signatures," recalls Cianfrocca. "Additionally Bayshore is fast enough to run in a network core in a network gateway. Plus the reporting we produce is much more detailed. Afterwards, one of the things they said to us was, 'we now know more about our network than our own network guys do.'"

The business case for the executive team manifested itself quickly. They attached a monetary value to the IP and were easily able to calculate ROI. As soon as a high-value piece of information was detected crossing a network boundary or going to an end-point that it wasn't supposed to be on, the solution paid for itself.

At the end of the roll out, the business advantages of the Bayshore SE solution were quite compelling: it provides unprecedented detail about the content of the network while preventing the loss of intellectual property.

ABOUT BAYSHORE NETWORKS

Bayshore Networks® is the cybersecurity leader for the Industrial Internet of Things. Our award-winning, patented IT/OT Gateway platform provides IT departments with unprecedented visibility into OT operations.

The Bayshore platform enables Fortune 1,000 industrial and enterprise customers to rapidly build and execute policies for OT cybersecurity, M2M communications, manufacturing operations, and robotics automation.

The Bayshore platform is distinguished by its extremely deep content inspection, granular filtering of network flows (including files within files and archives), policy building and enforcement, and its ability to detect, parse and segment industrial protocols. Leveraging these capabilities, Bayshore delivers ROI in areas such as production zone cybersecurity, operational continuity, data protection/data loss prevention, and plant safety.

The Bayshore platform deploys from the cloud, as a virtual machine, or as a gateway hardware appliance. Bayshore has strategic partnerships with leading technology companies including Cisco Systems and BAE Systems.

ABOUT THE INDUSTRIAL INTERNET CONSORTIUM

Bayshore Networks has been a member of the Industrial Internet Consortium (IIC) since May, 2014. The Industrial Internet Consortium is a global public-private organization of over 140 members, formed to accelerate the development, adoption and wide-spread use of interconnected machines and devices, intelligent analytics, and people at work. Founded by AT&T, Cisco, General Electric, IBM and Intel in March 2014, the Industrial Internet Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. Visit www.iiconsortium.org.