Bayshore Security & Operational Policy

Inside

Arista and Bayshore are providing a foundation for enterprise-wide policy regulation that applies to data centers, SDNs and clouds.

Layer 7 Content and Context Awareness

Bayshore Networks and Arista have collaborated to provide a foundation for enterprise-wide security and operational policy regulation, in the data center, SDN, or the cloud.

Arista EOSTM is designed to provide a foundation for the business needs of next-generation datacenters and cloud networks. The open, flexible Bayshore SETM (Secure Enterprise) platform enables you to quickly deploy, evaluate and enforce policies in EOS environments.

Bayshore's Layer 7 content and context aware technology implements advanced behavioral analysis, application discovery and profiling to help network administrators enforce security and access control policies. The ultra high-speed, multiprotocol technology is aimed at securing IT and operational technology networks in the network core. Benchmarked at faster than 10-Gbps, the solution is fast and flexible, providing content- aware filtering at line rate.

Bayshore's PallatonTM, an innovative policy-expression language, enables Bayshore SE to provide content inspection and policy enforcement at line rate.

Bayshore SE and Pallaton work in concert with Arista EOS. The Bayshore SE can plug directly into Arista data center switches at the TAP point or run virtually.

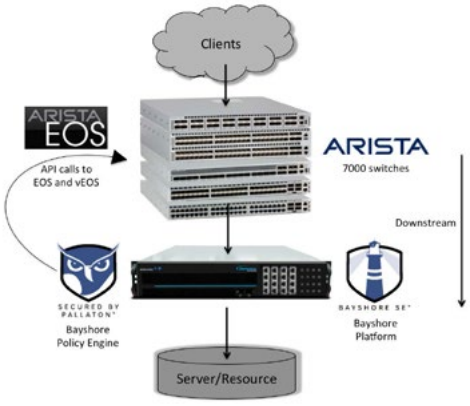

Figure 1: Bayshore Insertion Point. *The Bayshore SE platform resides downstream of Arista data center switches, inspecting Layer 7 traffic such as web flows and file shares. In this way, the solution changes policy dynamically, such as a user's access to resources, based on their behaviors.*

Pallaton: Deploy, Evaluate and Enforce Policy

The flexibility of the Pallaton language enables policies to be expressed uniformly across multiple device types and security categories (firewalls, application security, etc.). Pallaton rules are applied to streams of network device data and works in terms of actual wire protocols. Pallaton is so powerful that it is capable of expressing the requirements of different security functions. This enables different teams to coordinate and synchronize policy objects.

Pallaton works in a run-time context, inspecting web flows and file shares. The following features make it is easy to work with:

- Rules are created in a GUI and include policy objects from many protocols.
- Policies are expressed in terms of applications and users rather than in firewall rules or IDS signatures.
- The language is predicate-based and customizes to the specific context of the network.

EOS: Foundation for Business Needs

Bayshore SE and Pallaton work in concert with Arista EOS. The Bayshore SE can plug directly into Arista data center switches at the TAP point or run virtually. The extensibility of Pallaton enables policies to be dynamically changed based on user behaviors. For example, when detecting a security policy violation or APT, an outcome might be to re-direct a user to a honeypot network with an IDS that fingerprints his behavior.

Use Case: High-Value IP Data Protection

Because it inspects content at line rate, Bayshore SE mitigates rogue insider and APT threats to sensitive Intellectual Property in Arista data centers. While traditional DLP prevents sensitive content from crossing network boundaries, Bayshore provides unprecedented visibility and access control by evaluating the content moving through your network connections.

In IP Protection, the key differentiator is the platform's flexible policy evaluation. This flexibility enables you to track usage patterns and to create classifications by people, by document, by traffic, or even by metadata. You can create content around any of your classifications 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, and FTP sites. Pallaton rules are quickly configurable – particularly for organizations that already track their own data content categories. It inspects Layer 7 content and makes rules-based decisions dynamically, in real-time, enabling policy evaluation to become policy enforcement.

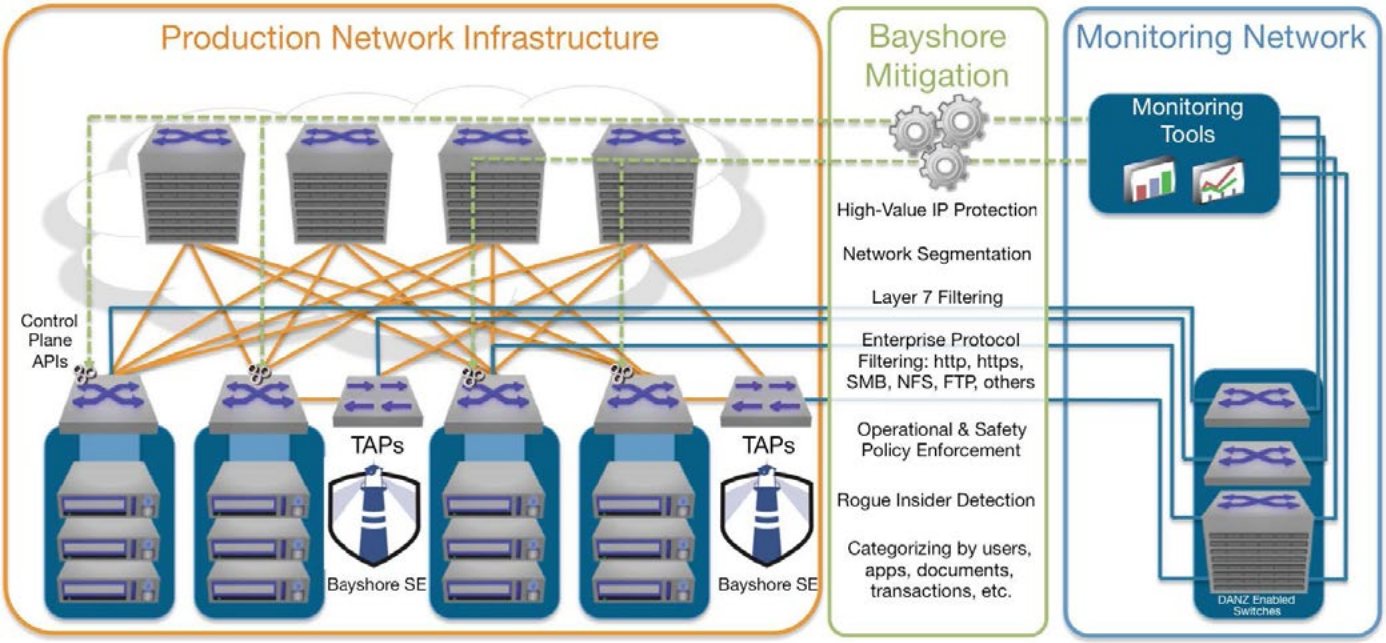

Figure 2: A Comprehensive Mitigation Solution. *Bayshore's Security and Operational Policy capabilities augment a robust set of mitigation capabilities for Arista switches.shares. In this way, the solution changes policy dynamically, such as a user's access to resources, based on their behaviors.*

Use Case: Layer 7 Network Segmentation

By operating at Layer 7, Bayshore's content awareness enables you to segment networks without disrupting the network topology. The Bayshore platform solves the problem of network segmentation according to Layer 7 privileges. To segment networks, Pallaton categorizes network streams in accordance with compliance-driven requirements that networks should remain segregated by business unit, geography, or both.

It provides real-time traffic categorization and endpoint device characteristic context, deployed on monitor ports or network taps. This content- and context-sensitivity is a key differentiator against legacy firewalls that segment networks at Layer 3. The platform leverages awareness of content and device-context parameters while overlaying on top of the Layer 3 topology.

With Bayshore SE, you can quickly configure policies that are much closer to the business rules you're actually trying to enforce. Significantly, this approach doesn't require you to make changes to your existing topology or security infrastructure.

Conclusion

When deployed in concert, the Bayshore platform plus Arista EOS aims to set the global standard for enterprise access control policy in mission-critical enterprise environments.

About Bayshore Networks

Bayshore Networks is setting the standard for operational, safety and security policy for the Internet of Things. Our award-winning, patented, industrial-strength cybersecurity platform is developed exclusively in the United States and is trusted by world leaders in Industrial Controls, Critical Infrastructure and Global Enterprises.

The open, flexible Bayshore platform provides a foundation for organization-wide policy execution. It enables you to quickly deploy, evaluate and enforce industry standards and customized application-layer policies that drive your business objectives. Bayshore's core technology is PallatonTM, an embedded, extensible, XML-based policy language.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office
1390 Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A & B, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062