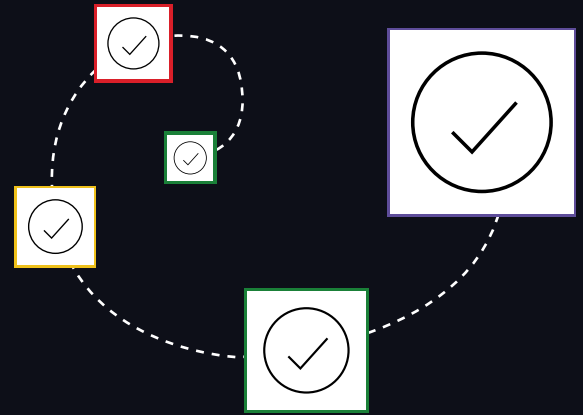


Streamlining FinTech Audit Data



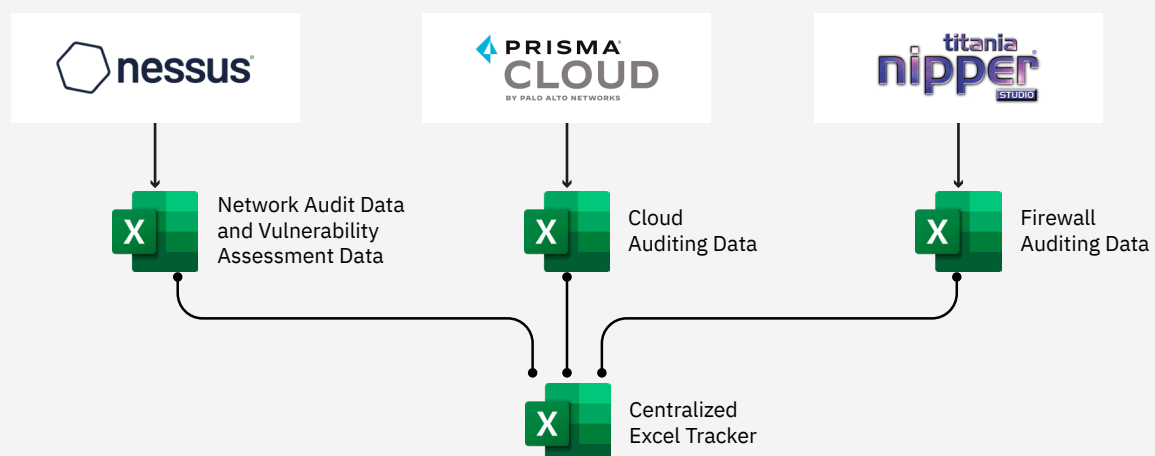
The Challenge

A large fintech company based in North America was attempting to provision their infrastructure to handle 1 million transactions a day. The company has a hybrid infrastructure using on-premises devices, managed data centers, and cloud providers. Since they are in the fintech industry and deal with personally identifiable information (PII), it is essential for them to meet many compliance requirements, including their primary obligation, PCI DSS.

Dealing with Audit Data Before Strobes

The organization has a decent security team and stakeholders who are responsible for various activities, such as vulnerability management, auditing infrastructure, network security, firewalls, databases, risk, and compliance. They purchased licenses for various tools to automate these activities, some of which are Nessus, Prisma Cloud, and Nipper.

This is how they originally handled their audit data:



A typical workflow included the following:

- Run bi-weekly vulnerability scans and network audit scans using Nessus.
- Run cloud auditing scans on Prisma cloud in real-time.
- Run real-time cloud auditing scans on the Prisma cloud.



- Collect data in Excel sheets and send it to the vulnerability management, risk, and compliance teams for aggregation.
- Aggregate issues, assign them to the appropriate resources, and re-run the scans to confirm whether the issues have been resolved.

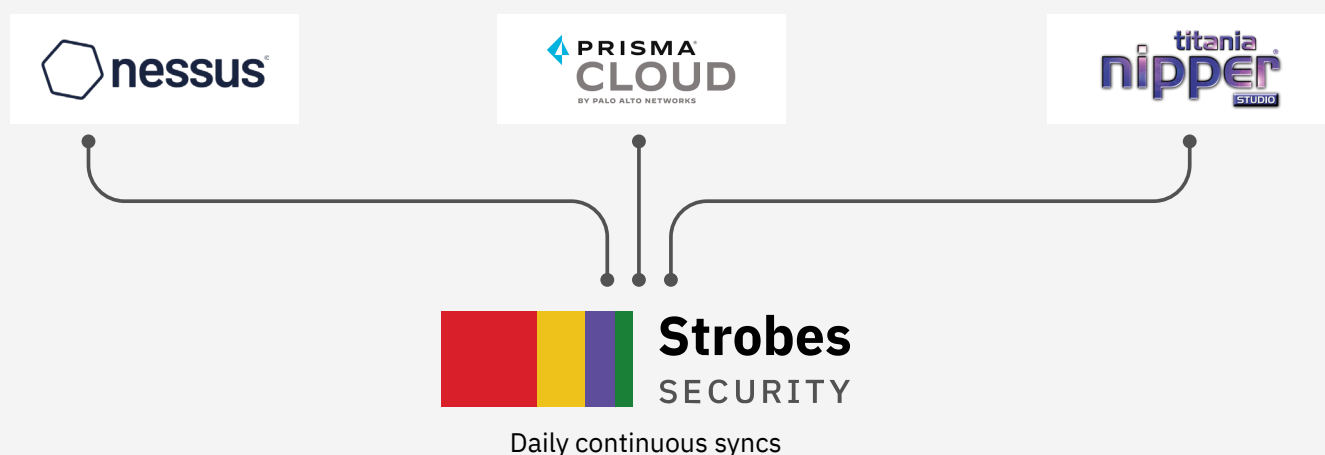
Their teams worked in silos, and there wasn't much cooperation making collaboration difficult and chaotic at times to holistically manage their environment. To overcome these challenges, the company started looking for an alternative. A centralized tool to automate inefficient work and make collaboration easier.

Dealing with Audit Data After Strobes

Strobes provided features to make their work easier and more efficient. Here are the most used features that reduced their workload by 50%.

Integrations

Strobes platform has ready-made integrations with Nessus, Prisma cloud, and Nipper. The customer simply used API keys to ingest audit data from the 3 different tools. Using daily syncs, the company kept its audit data up to date in a centralized place.



Asset & Risk Inventory

Strobes VM365 provided a centralized way to track and tag risks to all assets. As assets are audited on a regular basis, they are ingested in the platform where stakeholders can quickly filter and drill down to the most important ones.



An example of filtering assets and drilling down the most risky ones

Auditing & Vulnerability Management

The company now maintains an up-to-date, automatically deduplicated and prioritized list of vulnerabilities and audit data within the platform.

- With features, like
- Tagging
 - Assigning
 - Commenting
 - Attachments

Users can easily collaborate to identify the most important issues and work together to quickly patch them.

<input type="checkbox"/>	ID	Title	Severity	Status	Prioritization Score	Days old
<input type="checkbox"/>	324993	18.8.5.2 Ensure 'Turn On Virtualization Based Security: Select Platfor...	High	New	420	3 days ago
<input type="checkbox"/>	324992	18.8.5.3 Ensure 'Turn On Virtualization Based Security: Virtualization ...	High	New	420	3 days ago
<input type="checkbox"/>	324991	18.8.5.4 Ensure 'Turn On Virtualization Based Security: Require UEFI ...	High	New	420	3 days ago
<input type="checkbox"/>	324990	18.8.5.5 Ensure 'Turn On Virtualization Based Security: Credential Gu...	High	New	420	3 days ago
<input type="checkbox"/>	324989	18.8.5.7 Ensure 'Turn On Virtualization Based Security: Secure Launc...	High	New	420	3 days ago
<input type="checkbox"/>	324988	CIS_DC_SERVER_2019_Level_1_v1.3.0.audit from CIS Microsoft Win...	Medium	New	140	3 days ago
<input type="checkbox"/>	324987	2.3.7.6 Ensure 'Interactive logon: Number of previous logons to cach...	High	New	420	3 days ago
<input type="checkbox"/>	324986	2.3.10.4 Ensure 'Network access: Do not allow storage of passwords ...	High	New	420	3 days ago
<input type="checkbox"/>	324985	5.2 Ensure 'Print Spooler (Spooler)' is set to 'Disabled' (MS only)	High	New	420	3 days ago
<input type="checkbox"/>	324984	18.1.3 Ensure 'Allow Online Tips' is set to 'Disabled'	High	New	420	3 days ago
<input type="checkbox"/>	324983	18.4.5 Ensure 'MSS: (KeepAliveTime) How often keep-alive packets a...	High	New	420	3 days ago
<input type="checkbox"/>	324982	18.4.7 Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect ...	High	New	420	3 days ago

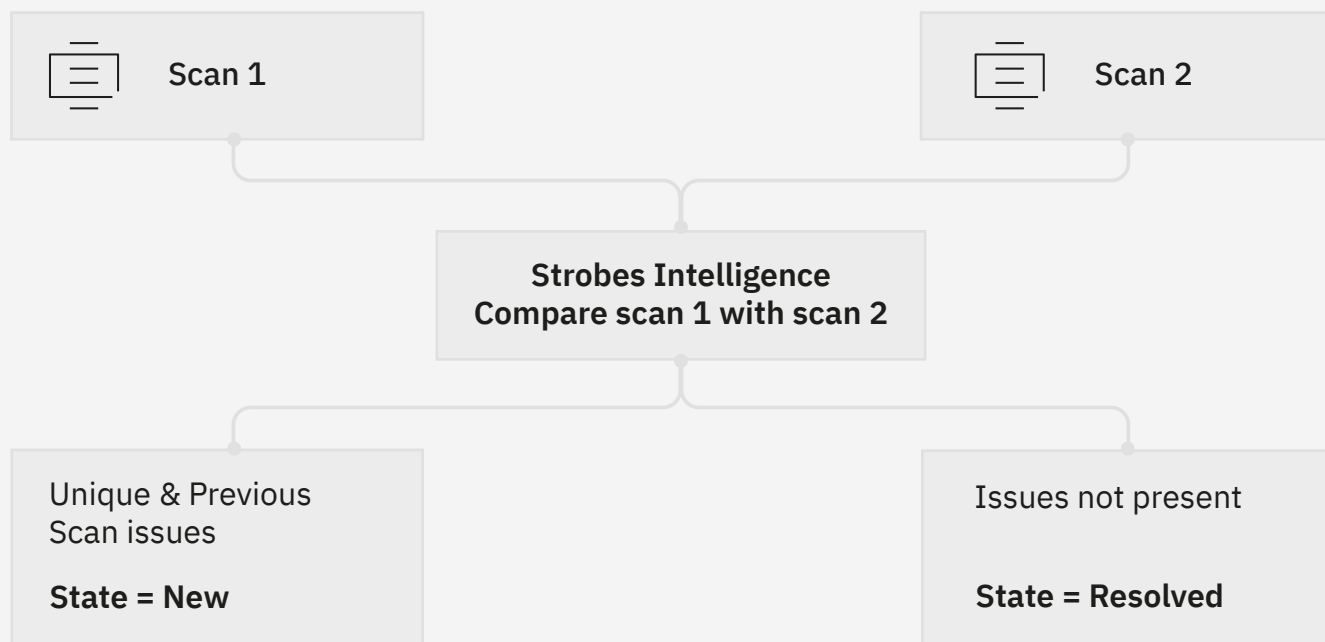
Items per page: 50 50 of many

A list of vulnerabilities that have been deduplicated and prioritized from all of the sources/scanners



Smart Closing

With daily syncs and scans, Strobes VM365 automatically compares scan results and identifies resolved issues, saving the customer a significant amount of time.

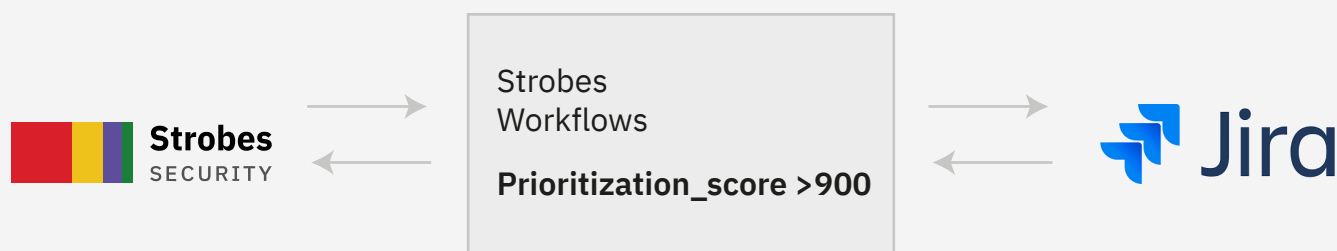


This image displays how Smartclose feature works inside Strobes

Workflow Sync with Jira

We created customized workflows to integrate issue-tracking tools like Jira, allowing them to receive the highest priority actions via Jira with a 2-way sync and Advanced QL that allows users to search using multiple conditional operators and multiple fields. Finally, they can drill down to particular results, which normally takes a lot of time.

Advanced QL & 2-way sync



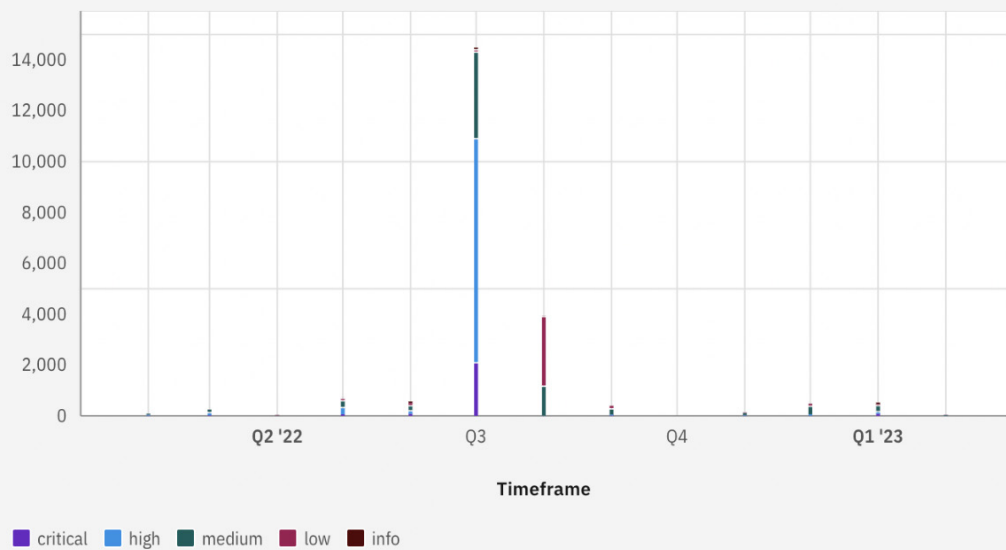


Reporting and Dashboarding

With access to 40+ customizable reports, the organization was able to increase transparency and improve its reporting to management.

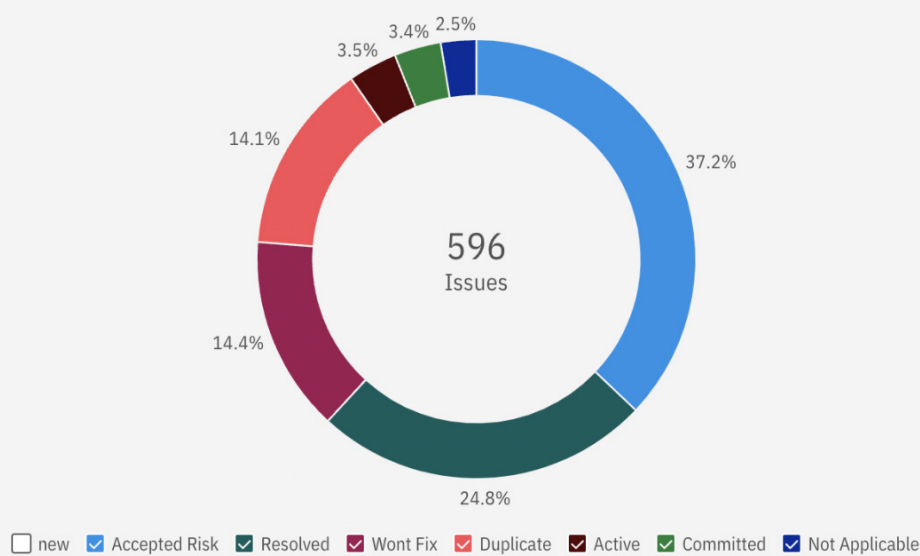
Here are three sample reports used by the organization.

Compliance Trend By Severity



The breakdown of vulnerabilities severity wise reported in a specific timeframe

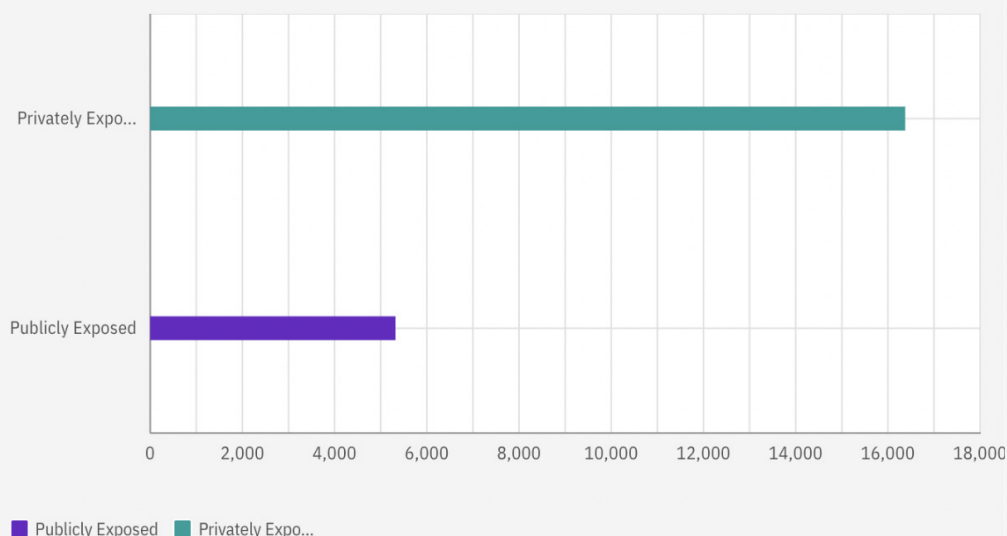
Issues By State



The breakdown of the state of vulnerabilities reported in a specific time frame



Issues By Exposure



The breakdown of the assets exposure-wise

Strobes ROI



50% lesser time spent to meet compliance



Seamless collaboration with teams



3x overall time savings



20% of costs reduction

Conclusion

Strobes provided the fintech company with a comprehensive and effective solution for managing its security posture and meeting PCI DSS compliance requirements. With its ability to aggregate and correlate audit data, prioritize resolution efforts, and provide a unified console, Strobes helped the company streamline its compliance efforts and improve its overall security posture.



United States (HQ)



5700 Tennyson Parkway, Suite 372, Plano, Texas 75024