© 2019 SPLUNK INC.

splunk>

Breaking Free From Legacy GRC

Achieving real-time integrated risk visibility

Matt Coose
CEO | Qmulos

Anthony Perez
Director of Public Sector Field Technology | Splunk

© 2019 SPLUNK INC.

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

© 2019 SPLUNK INC.

One Size Does Not Fit All

Every organization is at a different state of maturity

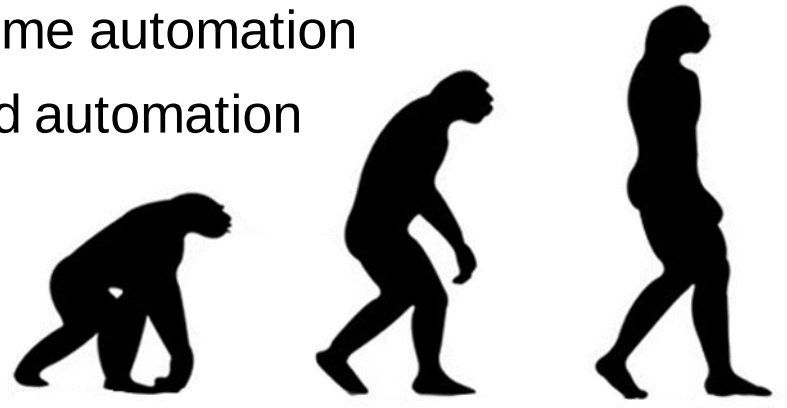
splunk> .conf19

© 2019 SPLUNK INC.

One Size Does Not Fit All

Different organizations are in different places

- Compliance and risk frameworks may be consistent across organizations
- Even when consistent, every organization has different needs based on their maturity
- Organizational maturity states may include:
  - Crawl: Basic processes, manual evidence, but limited visibility
  - Walk: Limited real-time insights and reporting visibility – some automation
  - Run: Comprehensive near real-time insights, reporting, and automation



© 2019 SPLUNK INC.

One Size Does Not Fit All

Different organizations are in different places

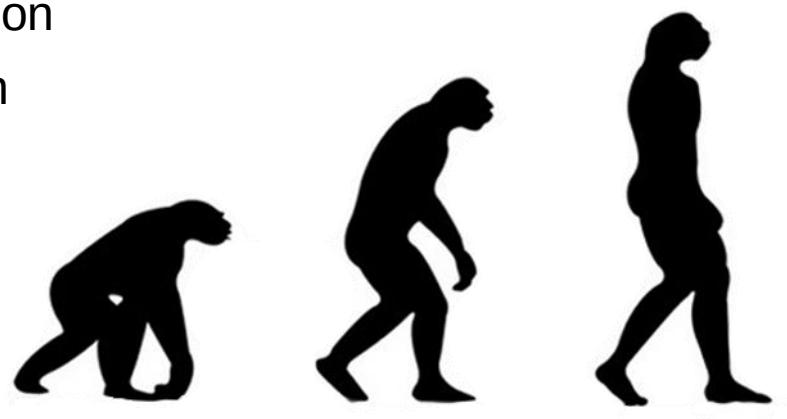
Compliance and risk frameworks may be consistent across organizations

Even when consistent, every organization has different needs based on their maturity

Organizational maturity states may include:

- Crawl: Basic processes, manual evidence, but limited visibility
- Walk: Limited real-time insights and reporting visibility – some automation
- Run: Comprehensive near real-time insights, reporting, and automation

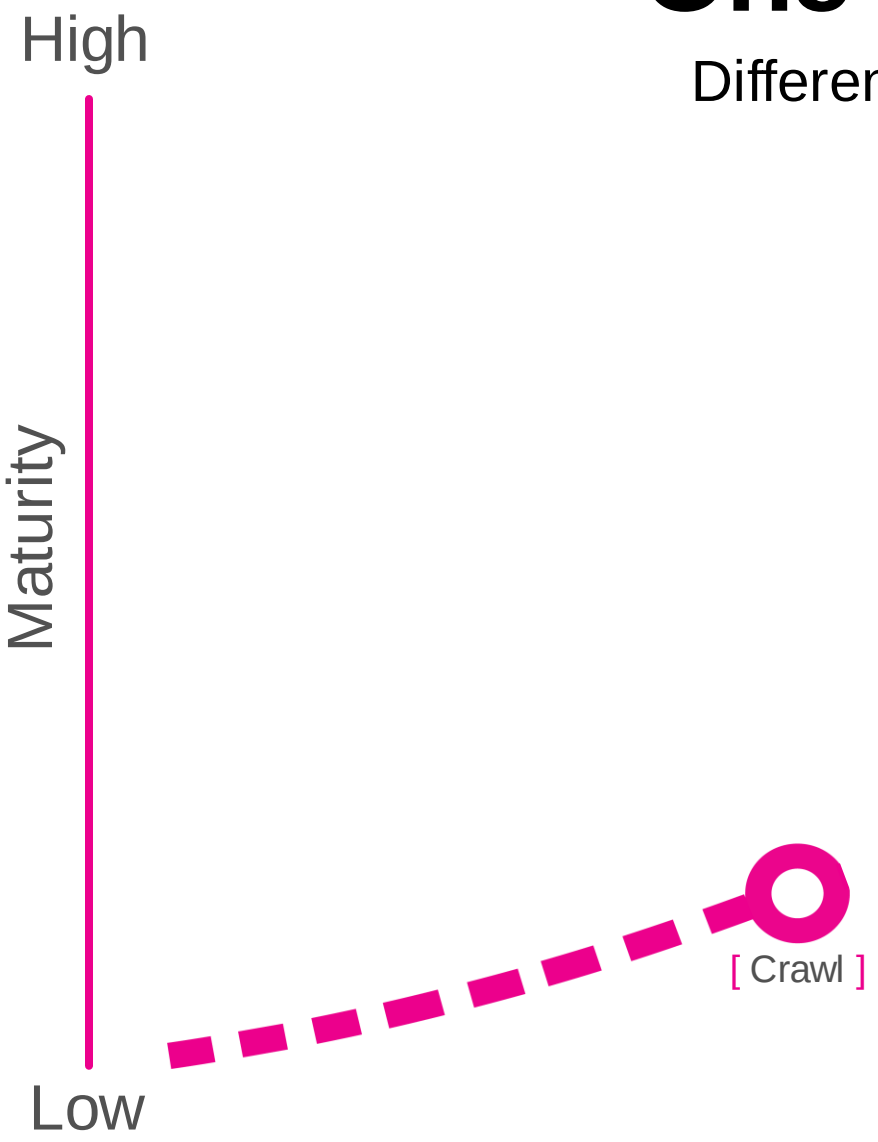
Finally, a quick and completely unscientific poll



© 2019 SPLUNK INC.

One Size Does Not Fit All

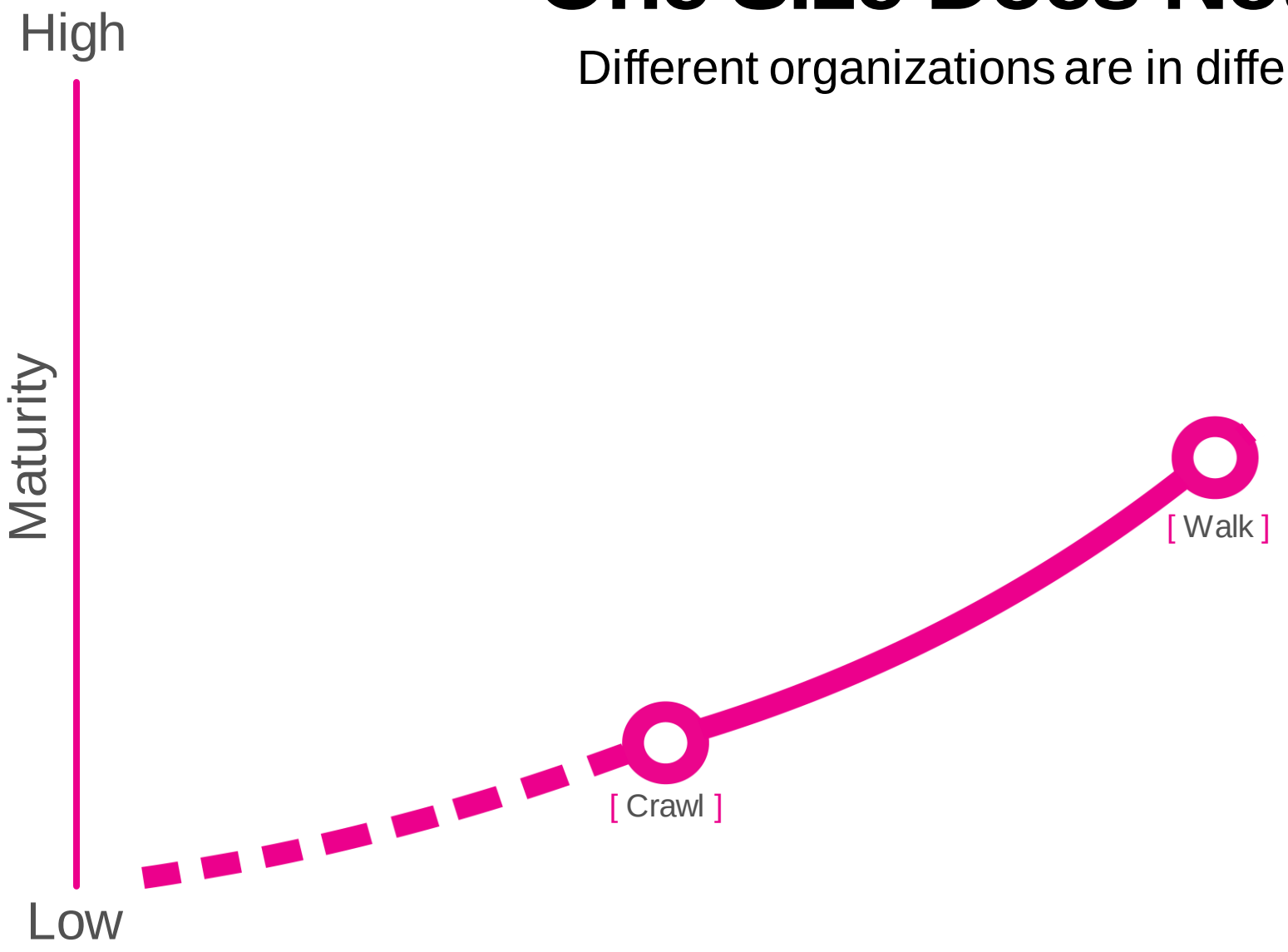
Different organizations are in different places



© 2019 SPLUNK INC.

One Size Does Not Fit All

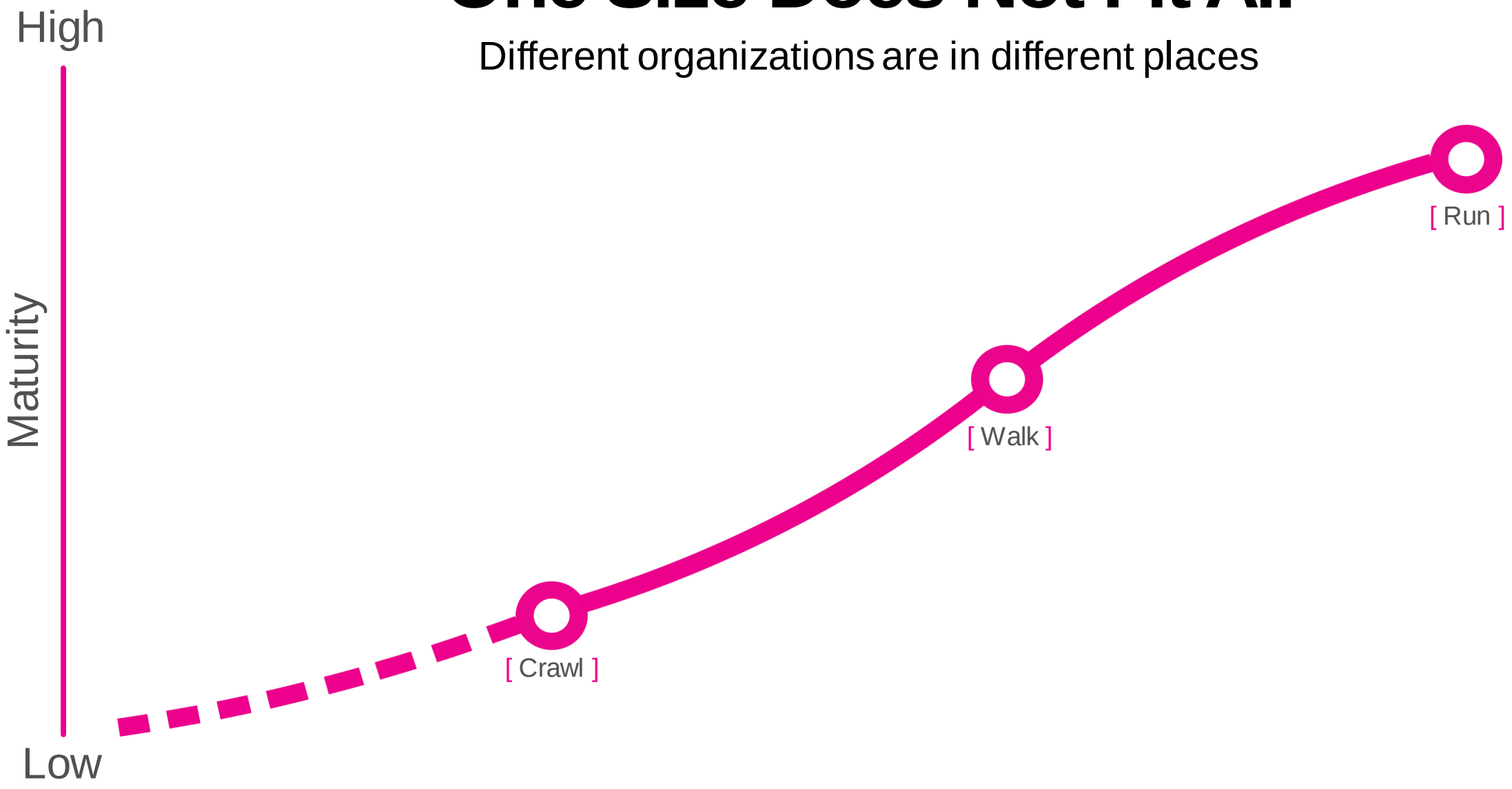
Different organizations are in different places



© 2019 SPLUNK INC.

One Size Does Not Fit All

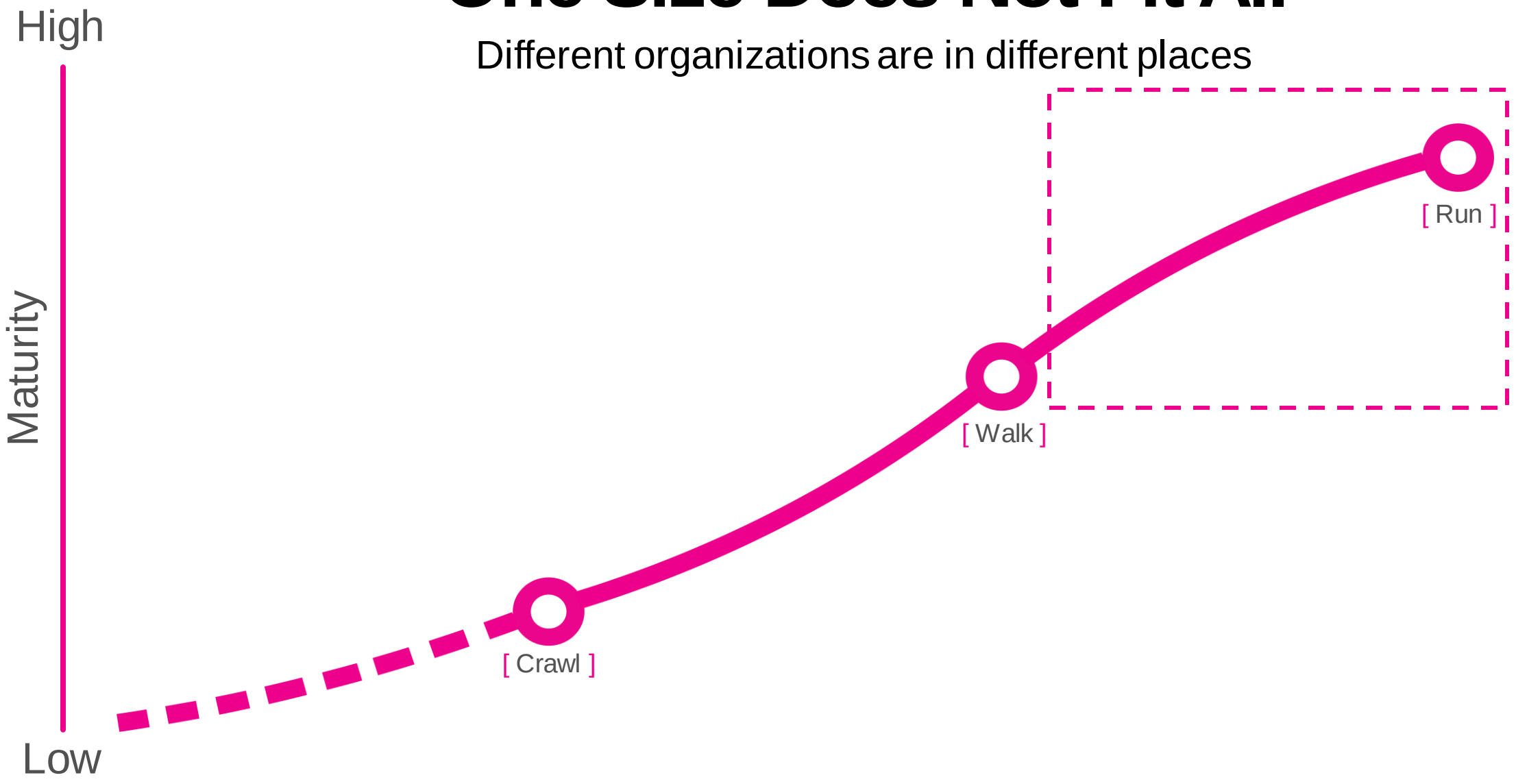
Different organizations are in different places



© 2019 SPLUNK INC.

One Size Does Not Fit All

Different organizations are in different places



© 2019 SPLUNK INC.

Consistently Inconsistent

Common obstacles to success with legacy GRC tools

splunk> .conf19

© 2019 SPLUNK INC.

Consistently Inconsistent

Common obstacles to success with legacy GRC tools

Scope and Scale

- Multiple systems, organizations, sub-organizations, and locations of various structures and sizes
- High frequency of events and high volume of data
- Real-world performance of legacy GRC solutions struggles to keep up

© 2019 SPLUNK INC.

Consistently Inconsistent

Common obstacles to success with legacy GRC tools

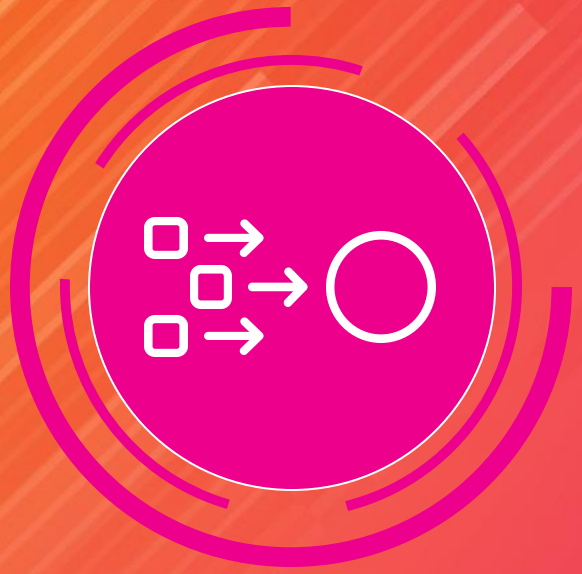
Visibility

- Visualization capabilities of legacy GRC solutions often fail at larger scales
- Representation of organizations, systems, and security posture is commonly outdated or slow
- Actual security and compliance posture can be unclear

© 2019 SPLUNK INC.

Consistently Inconsistent

Common obstacles to success with legacy GRC tools



Diversity

- Multiple systems, vendors, geographic locations, organizations, and data formats create significant complexity
- This complexity is nearly impossible to normalize effectively using legacy GRC solutions
- This normalization challenge is an additional contributor to the “Visibility” challenge

© 2019 SPLUNK INC.

Consistently Inconsistent

Common obstacles to success with legacy GRC tools

Retroactive

- Data latency and system slowness injects analytic lag
- Analytic lag means that analysts and information system security officers (ISSOs) are constantly looking at stale data
- This prevents genuine data-driven decision making and real-world continuous monitoring (CONMON)

© 2019 SPLUNK INC.

Consistently Inconsistent

Common obstacles to success with legacy GRC tools

Rigidity

- Constantly evolving technology ecosystems drive a need for frequent up-keep and modifications to legacy GRC solutions
- This need for up-keep and modifications commonly drive high maintenance and extension costs
- While these extensions and modifications are underway, organizations face blind-spots in their CONMON

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

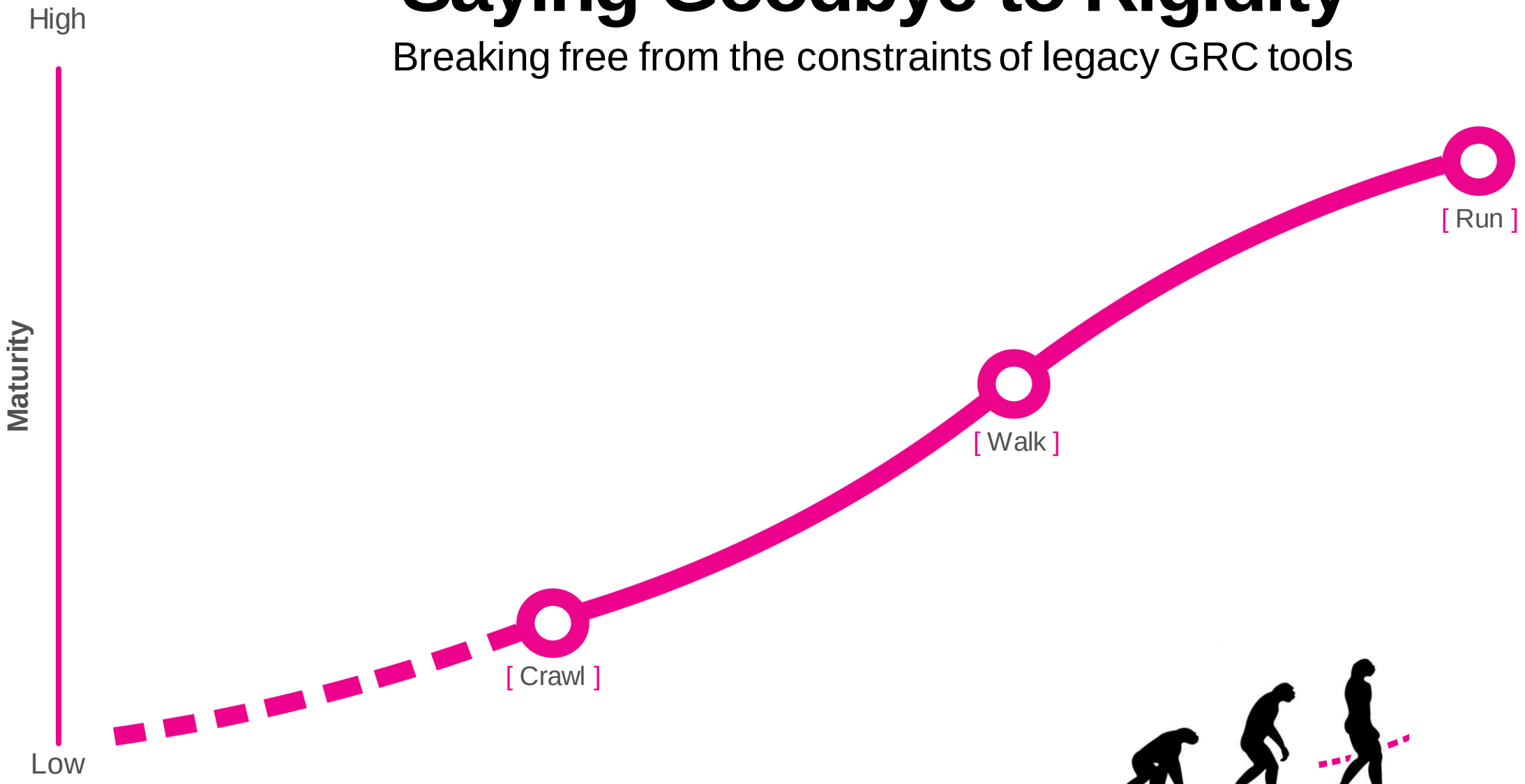
Breaking free from the constraints of legacy GRC tools

splunk> .conf19

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools

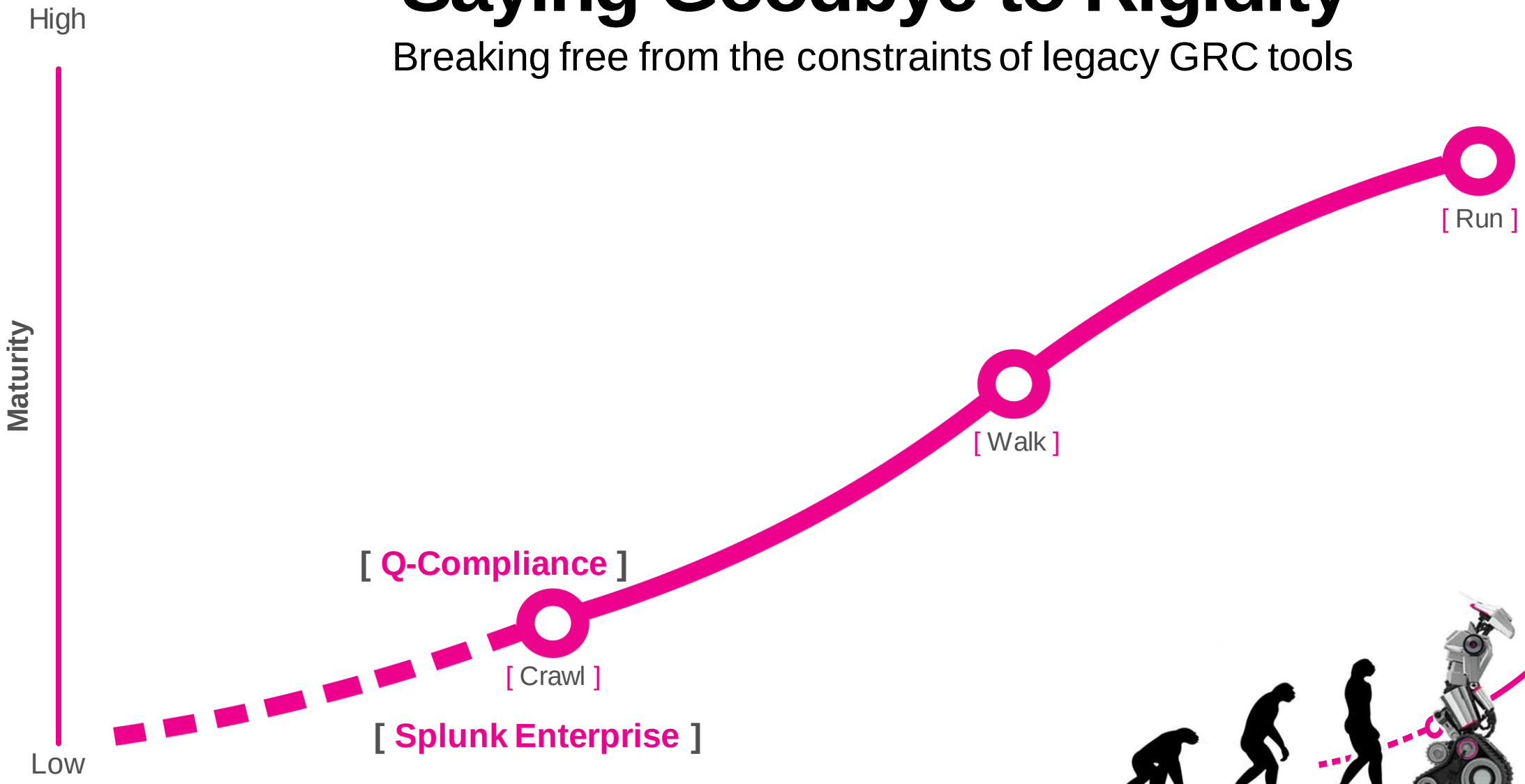


splunk> .conf19

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools

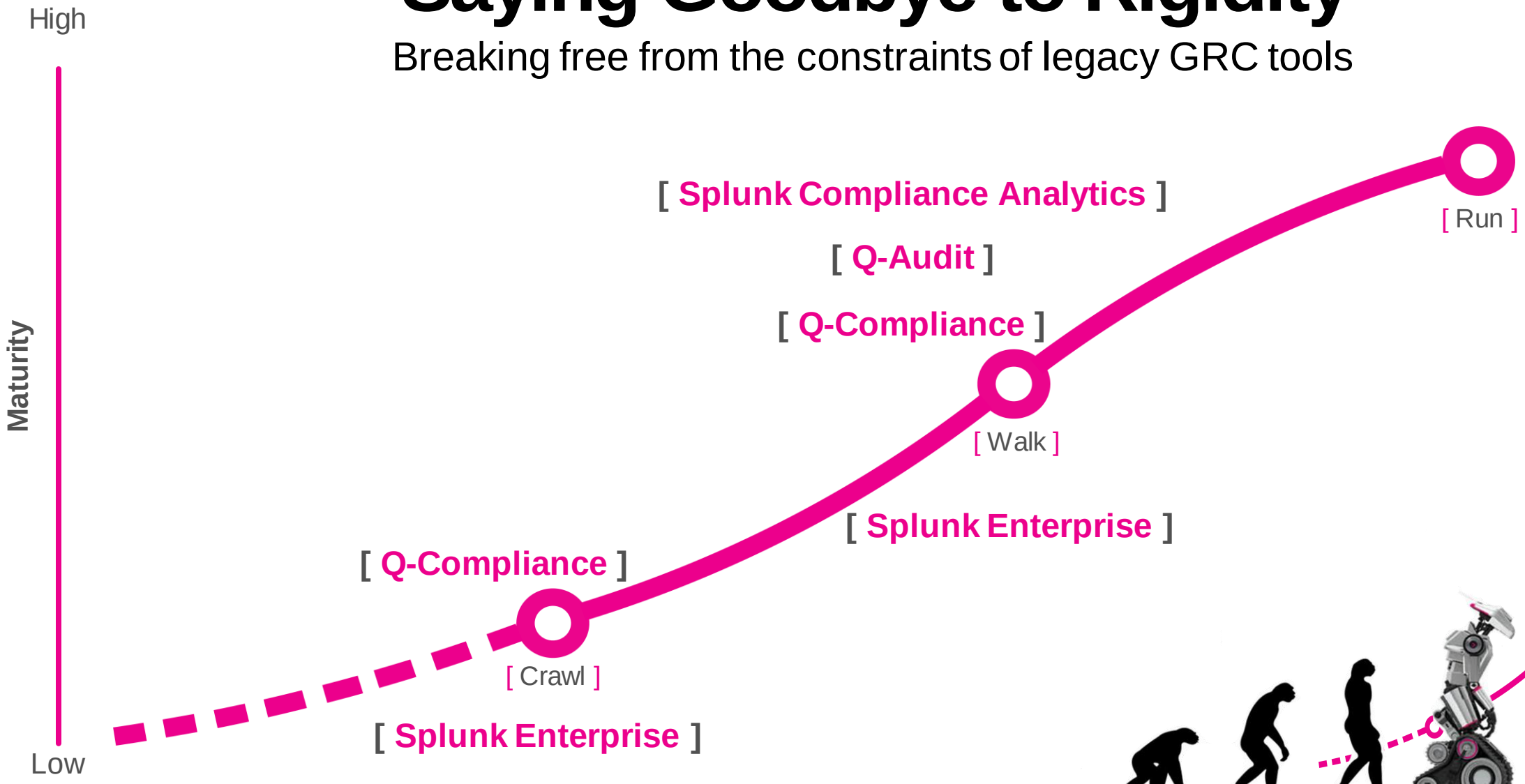


splunk> .conf19

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools



splunk> .conf19

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Breaking free from the constraints of legacy GRC tools

High

Maturity

Low

[Crawl]

[Q-Compliance]

[Splunk Enterprise]

[Walk]

[Q-Compliance]

[Splunk Compliance Analytics]

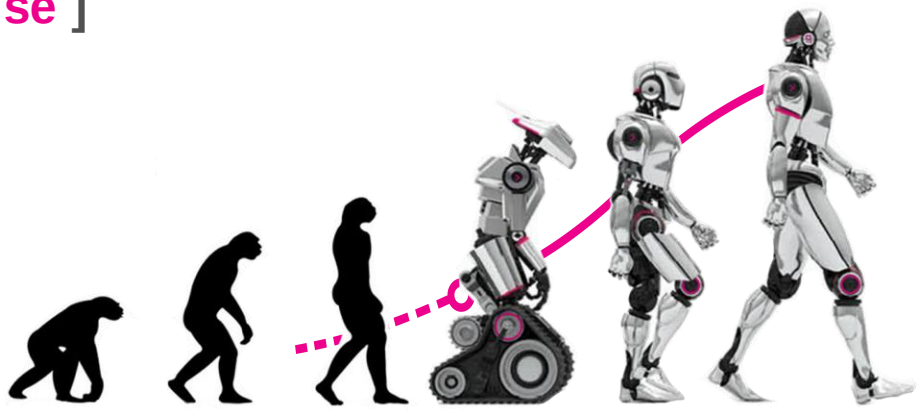
[Q-Audit]

[Splunk Enterprise]

[Run]

[Q-Compliance]

[Splunk Enterprise]



© 2019 SPLUNK INC.

Let’s revisit those legacy obstacles

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC

Scope and Scale

Historical Challenge	Breaking free with Splunk/Qmulos
✗ Multiple systems, organizations, sub-organizations, and locations of various structures and sizes	▪ Native tagging and lookup functionality enables org-specific data identification
✗ High frequency of events and high volume of data are often processing challenge	▪ Distributed architecture – on-prem, cloud, or hybrid ensure that performance can scale with real-world needs
✗ Real-world performance of legacy GRC solutions struggles to keep up	▪ Big-data architecture highly-performant at multi-Petabyte scale

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC

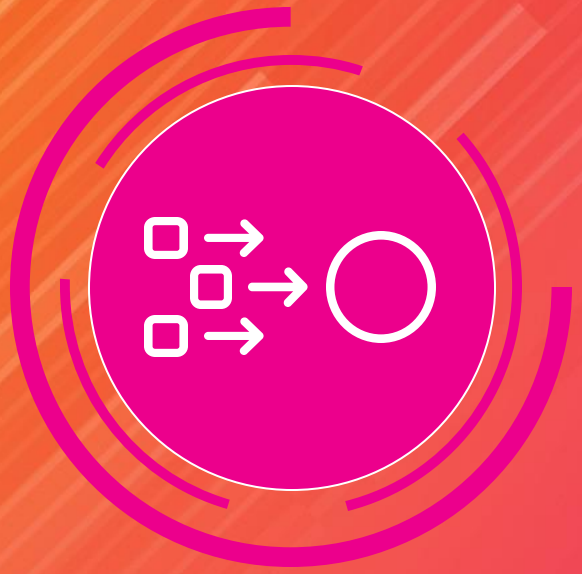
Visibility

Historical Challenge	Breaking free with Splunk/Qmulos
✗ Visualization capabilities of legacy GRC solutions often fail at larger scales	▪ Holistic visibility of even very-large data sets is enabled by the platform and a breadth of visualization layouts
✗ Representation of organizations, systems, and security posture is commonly outdated or slow	▪ Near real-time architecture ensures that security posture visibility is current and representative of the operating environment
✗ Actual security and compliance posture can be unclear	▪ Wide variety of highly flexible visualizations combined with near real-time data flows drive visibility and insight

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC



Diversity

Historical Challenge	Breaking free with Splunk/Qmulos
✗ Multiple systems, vendors, geographic locations, organizations, and data formats create significant complexity	▪ Vendor, data, location and format agnostic
✗ This complexity is nearly impossible to normalize effectively using legacy GRC solutions	▪ If the data exists in a human-readable form and you have access to it, you can analyze it
✗ This normalization challenge is an additional contributor to the “Visibility” challenge	▪ Native data normalization through common information models

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC

Retroactive

Historical Challenge	Breaking free with Splunk/Qmulos
✗ Data latency and system slowness injects analytic lag	▪ Analytic insights on timelines typically measured in milliseconds or seconds
✗ Analytic lag means that analysts and ISSOs are constantly looking at stale data	▪ Near real-time visibility prevents a false sense of security that may be created by stale data
✗ This is prevents data-driven decision making and real-world CONMON	▪ Executives and security leaders are genuinely empowered to make data-driven decisions for their orgs

© 2019 SPLUNK INC.

Saying Goodbye to Rigidity

Revisiting common obstacles to success with legacy GRC

Rigidity

Historical Challenge	Breaking free with Splunk/Qmulos
✗ Constantly evolving technology ecosystems drive a need for frequent up-keep and modifications to legacy GRC solutions	▪ Data source abstraction through common information models provide a highly flexible foundation
✗ This need for up-keep and modifications commonly drive high maintenance and extension costs	▪ Platform agility and vendor agnostic analytic / visualization framework is inherently flexible
✗ While these extensions and modifications are underway, organizations face blind-spots in their CONMON	▪ Platform flexibility and architecture are inherently resilient and naturally well-suited for CONMON and real-world computer network defense

© 2019 SPLUNK INC.

Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility

splunk> .conf19

Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility – ***Splunk Compliance Analytics***

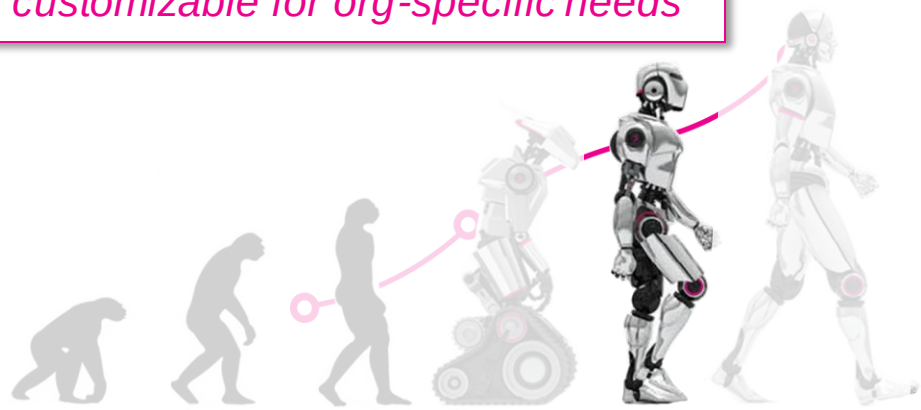
Splunk Enterprise + Splunk Compliance Analytics provide a quick-start solution

SCA provides a path to rapidly jump up the maturity curve and offers extensibility

- This is a great starting point for technical control monitoring, but it is not the top-tier of the maturity curve
- Your organization may require more out-of-the-box

Key Features:

- *Provides a quick-start way to rapidly jump up the maturity curve*
- *Baseline technical controls for near real-time visibility*
- *tstats-based searches for performance*
- *Easily scalable / customizable for org-specific needs*



© 2019 SPLUNK INC.

DEMO

© 2019 SPLUNK INC.

Giant Leaps Toward Maturity

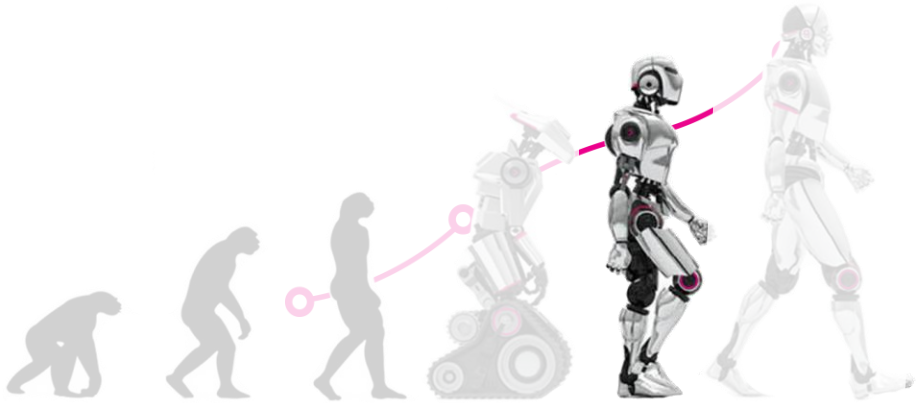
Achieving real-time integrated risk visibility – *Qmulos Q-Audit*

- Contextualization of logs is highly valuable
- Q-Audit enables a deep-dive into audit controls
  - Provides prescriptive audit policy (ICS 500-27) and analytics to monitor them – out of the box

Key Insights:

- *A lot of organizations use Splunk to just store audit logs*
- *Q-Audit takes things to a whole different level*
  - *Shows what you should log*
  - *How to monitor those logs and alert in real time*
  - *Enables actual monitoring of users and device activity*
- *This ensures that your org is fulfilling the actual purpose of audit controls*

- Tough part is mapping the vendor-specific event codes to the audit policy and auditable event categories



© 2019 SPLUNK INC.

Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility – *Qmulos Q-Audit*

- Contextualization of logs is highly valuable
- Q-Audit enables a deep-dive into audit controls
  - Provides prescriptive audit policy (ICS 500-27) and analytics to monitor them – out of the box

Key Insights:

- *A lot of organizations use Splunk to just store audit logs*
- *Q-Audit takes things to a whole different level*
  - *Shows what you should log*
  - *How to monitor those logs and alert in real time*
  - *Enables actual monitoring of users and device activity*
- *This ensures that your org is fulfilling the actual purpose of audit controls*

- Tough part is mapping the vendor-specific event codes to the audit policy and auditable event categories

"Here's what you should be logging"

"Here's how to monitor those logs and alert on them in real-time"

"You're not just checking the logs, you're actually monitoring the user and device activities on your network – This is actually the purpose of the audit and control activities in the first place"

© 2019 SPLUNK INC.

DEMO

© 2019 SPLUNK INC.

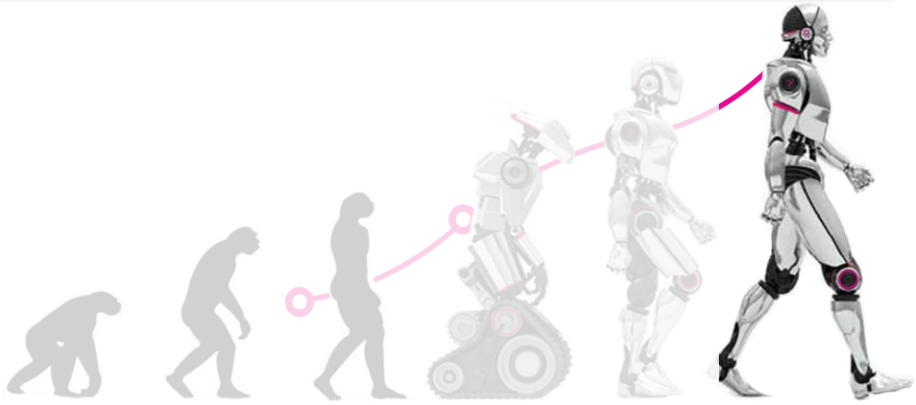
Giant Leaps Toward Maturity

Achieving real-time integrated risk visibility – ***Qmulos Q-Compliance***

- Q-compliance is a wholly new paradigm for integrated risk visibility
- Key functionality expected from GRC, but built on a big-data platform
- User interface to set up the environment across the full risk management process
- Dashboards, workflows, alerts, and POAMs to manage operational compliance activities
- Assess, audit, and monitor all controls – including technical and custom controls

Key Features:

- *Complete control sets and numerous frameworks*
- *Multi-level organizational hierarchies*
- *Multi-tenant organization based access control*
- *System boundaries and control inheritance*
- *Built-in control baselines and various overlays*
- *Custom controls and control overlays*
- *Hundreds of pre-built control analytics*
- *Supports all three types of evidence*
- *Automated control assessments*



© 2019 SPLUNK INC.

DEMO

What Do You Want Out Of a Capability?

Choosing the best fit for your organization

Maturity	Capability Highlights	Splunk Compliance Analytics*	Q-Audit*	Q-Compliance*
Run (Complete)	• Enables ongoing assessment and continuous monitoring of virtually all technical controls and custom controls • Enables automated assessment of technical controls • Create automated actions to detect, report and respond to compliance findings • Automate multiple compliance standards and frameworks			
Walk (Partial)	• Enables monitoring of basic cyber hygiene technical controls such as HWAM/SWAM/VUL/CSM (Q-Compliance) • Enables monitoring of Audit (AU) related controls (Q-Audit) • Enables monitoring of various technical controls (SCA)			
Crawl (Manual)	• Cost effective legacy GRC capabilities • Manually perform and capture audit/assessment results • Score compliance posture of systems • Define assessment boundaries and control baselines • Manual evidence collection and upload • Capture compliance work history and POAMs • Generate compliance artifacts (e.g. SSPs) • Establishes foundational architecture for centralized and/or federated technical data collection			

*All solutions require Splunk Enterprise

© 2019 SPLUNK INC.

So now what?

Next steps recommendations

1. Figure out where you are on the curve. Take the free Qmulos Readiness Assessment: www.qmulos.com/getready

2. Build it from scratch or talk to Splunk / Qmulos (Booth 109) for the solution that fits your organization (crawl, walk, or run).

3. Start doing compliance in a way that delivers real operational security value!

© 2019 SPLUNK INC.

Q&A

Matt Coose | CEO, Qmulos
Anthony Perez | Director of Public Sector Field Technology, Splunk

splunk> .conf19

© 2019 SPLUNK INC.

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION

© 2019 SPLUNK INC.

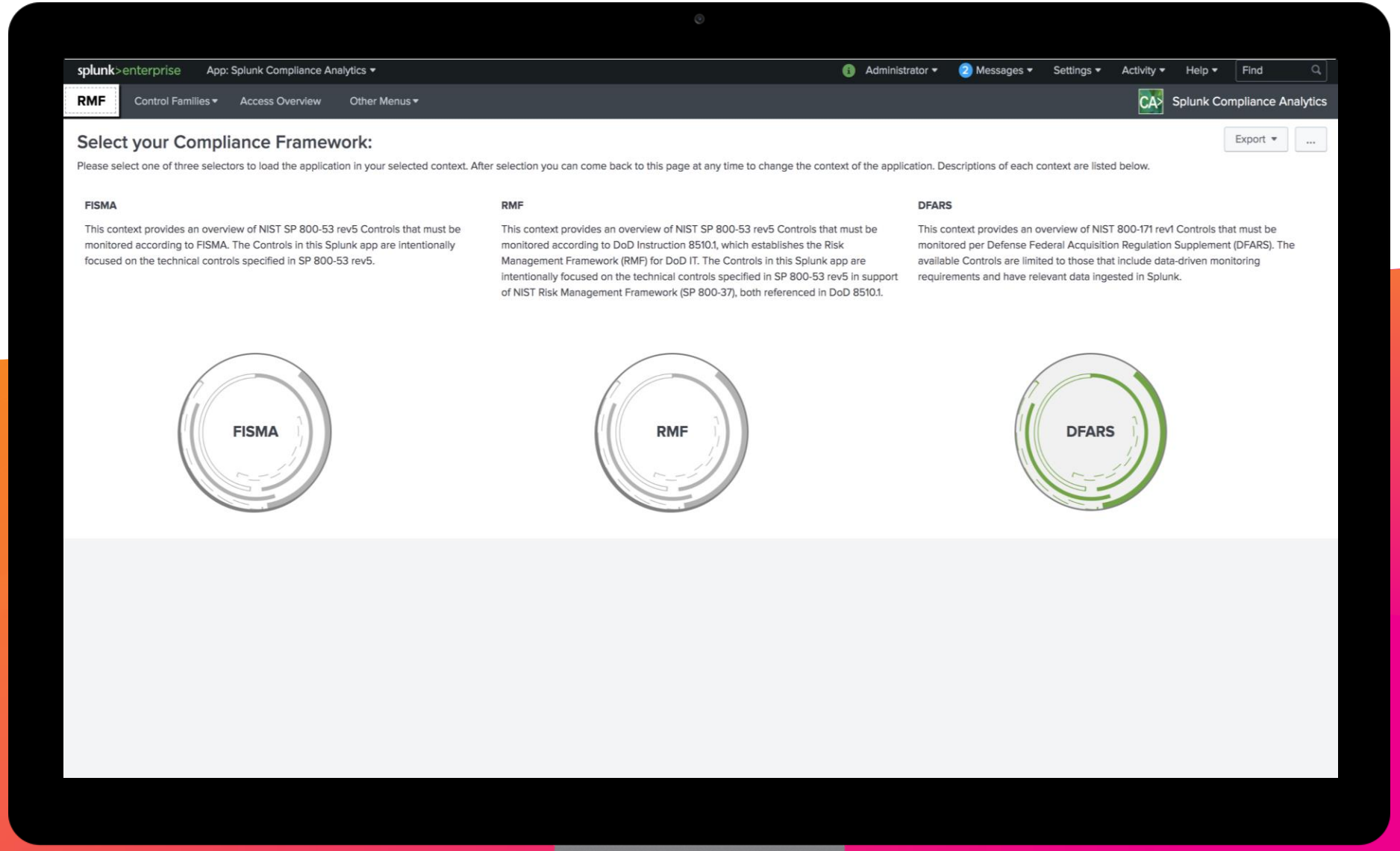
Backup

splunk> turn data into doing™

© 2019 SPLUNK INC.

Splunk Compliance Analytics

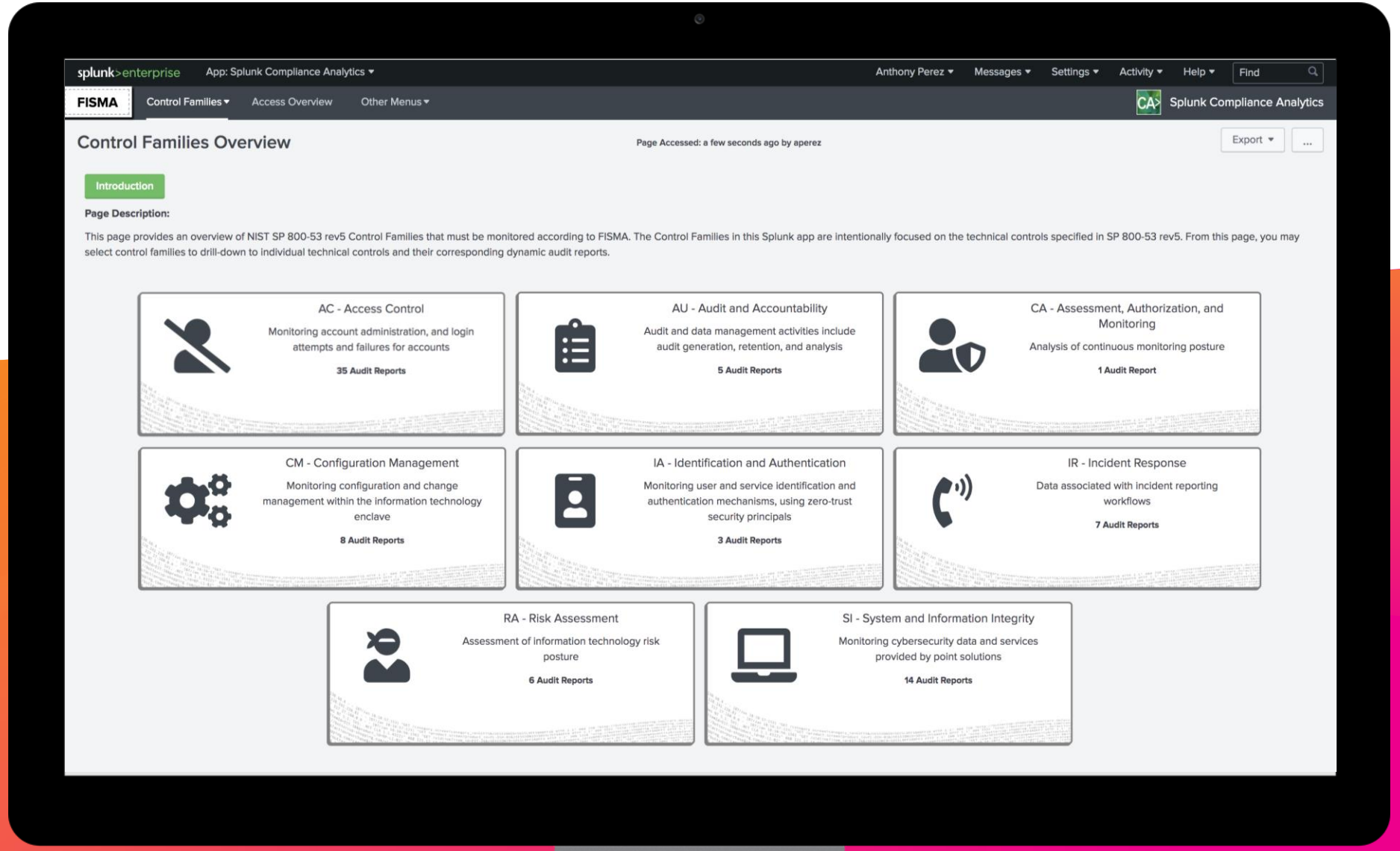
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

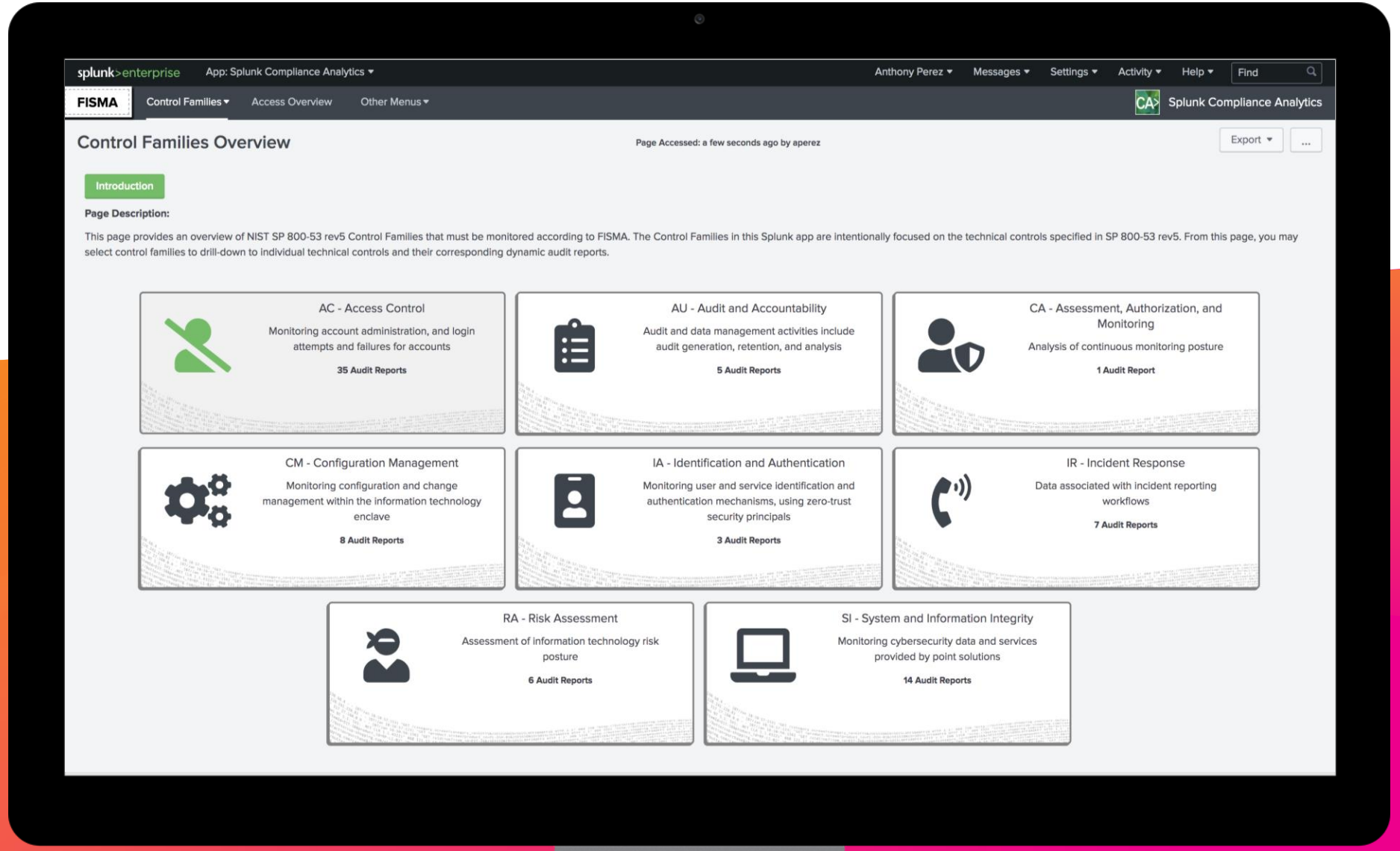
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

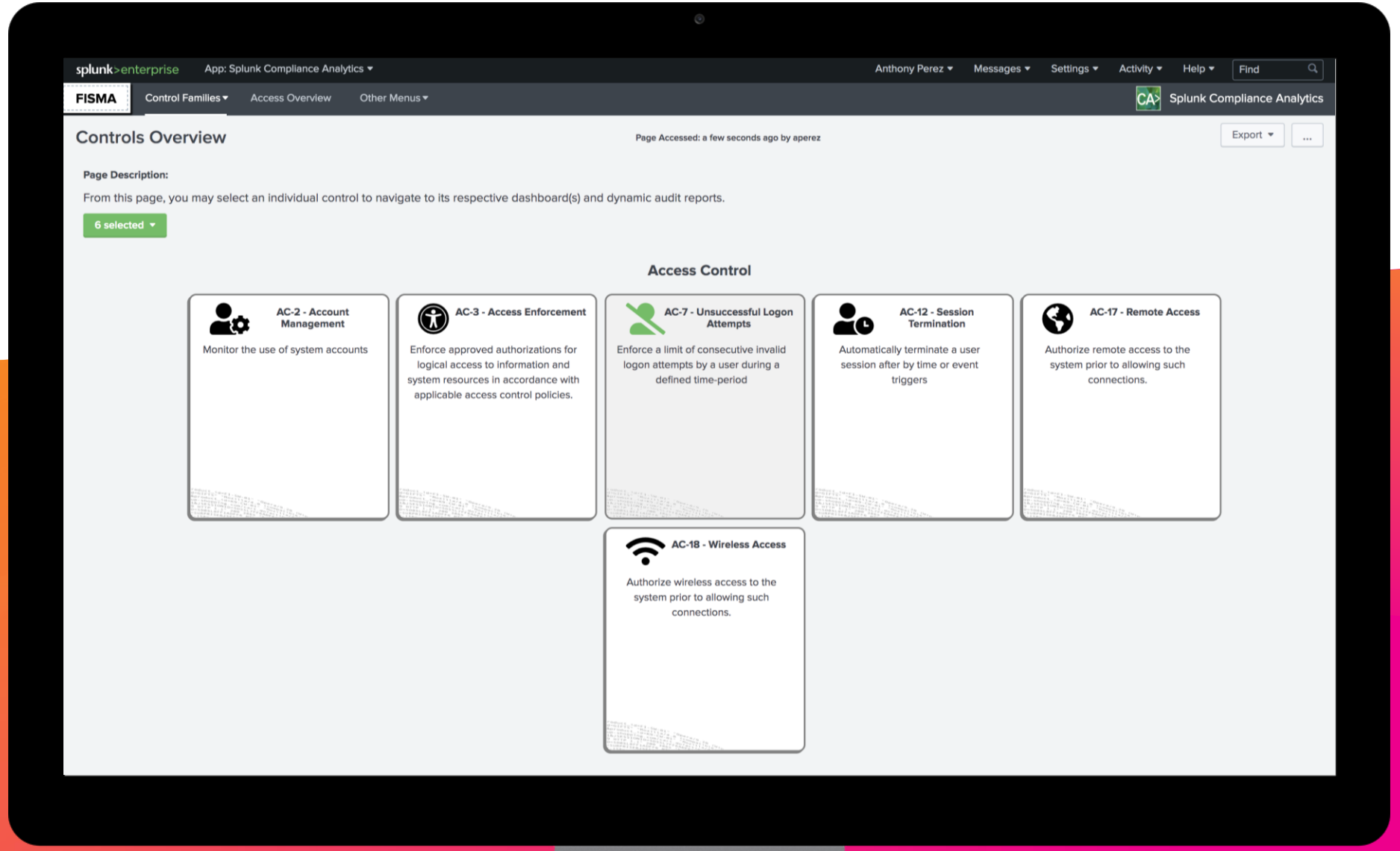
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

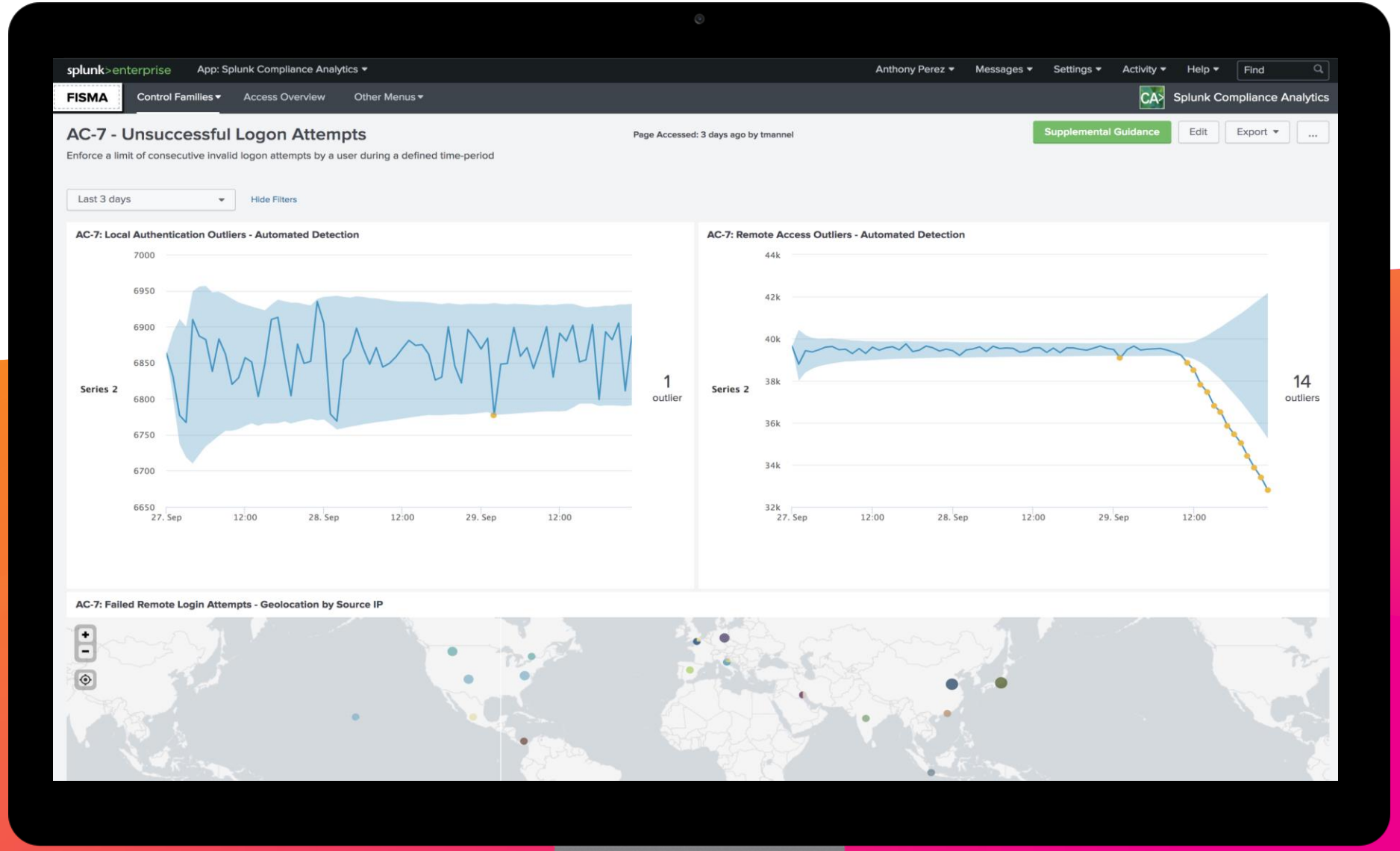
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

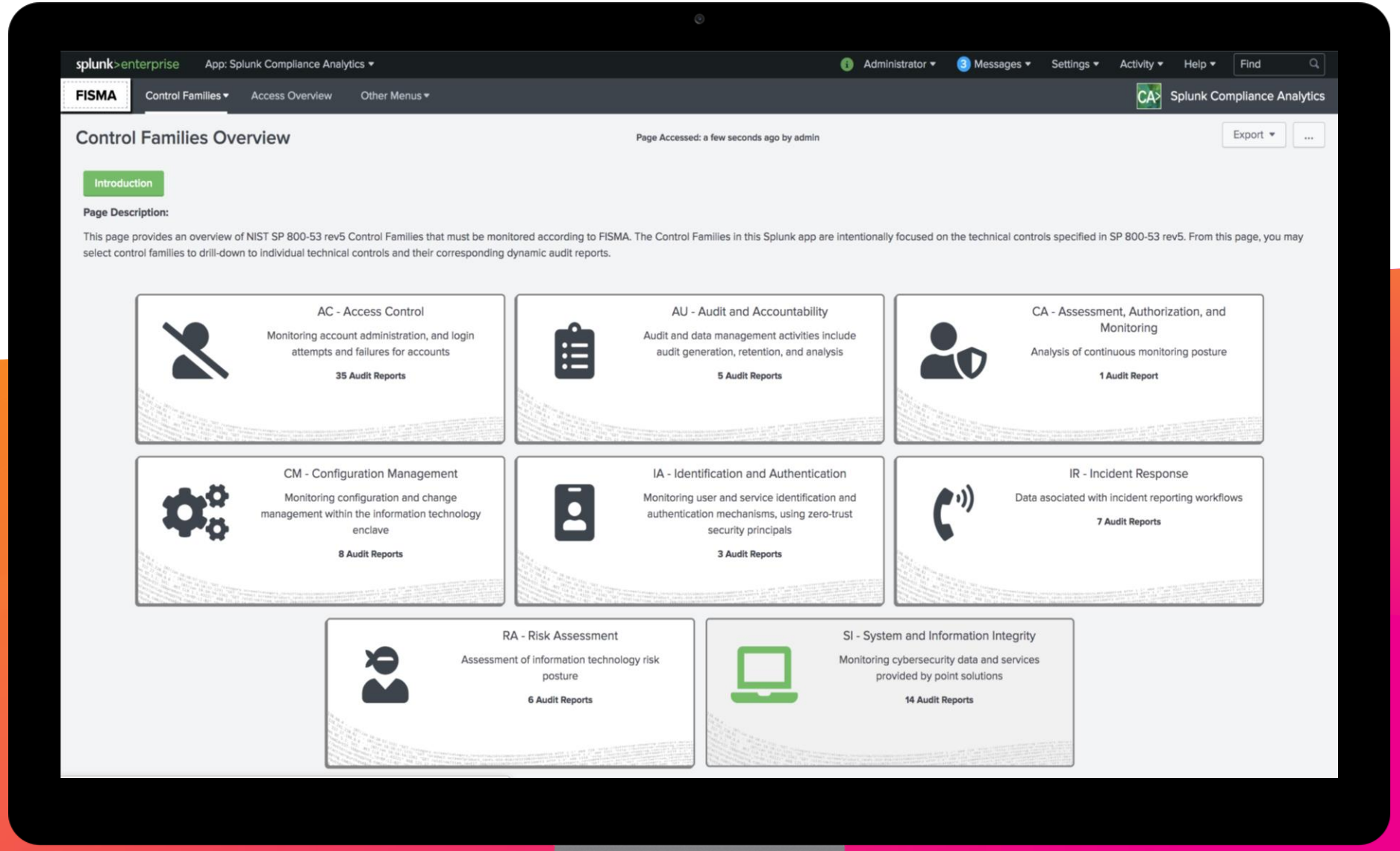
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

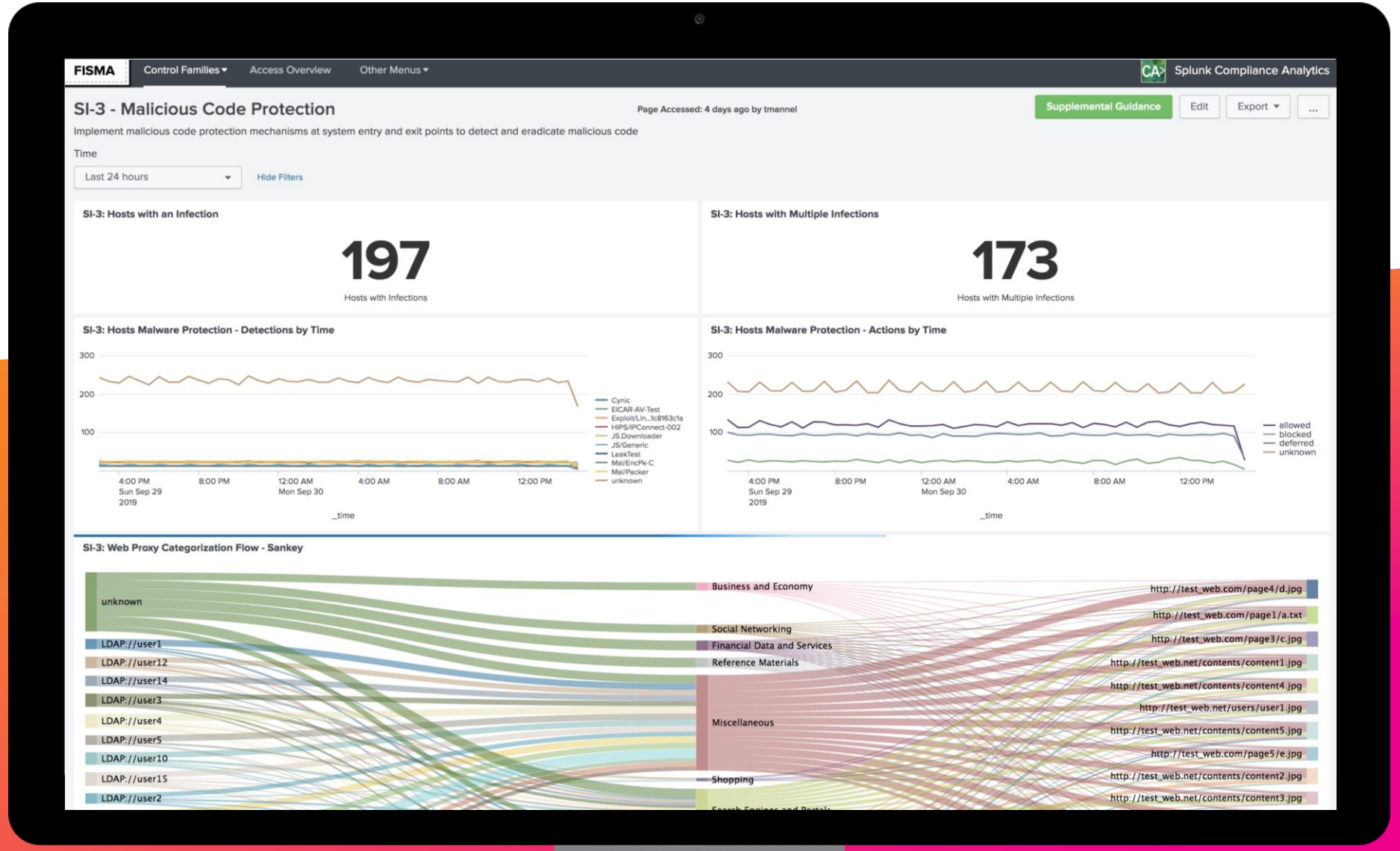
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

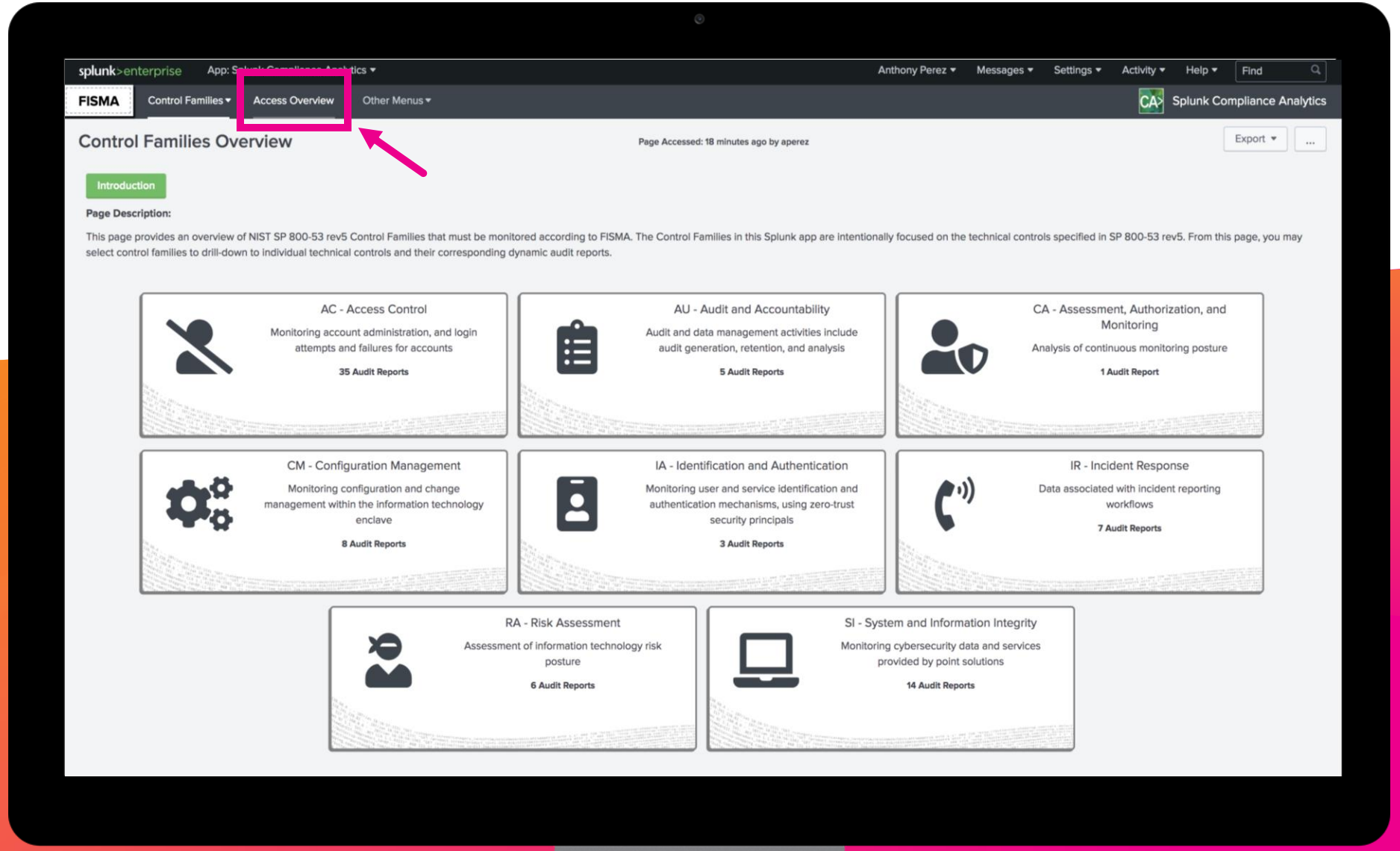
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

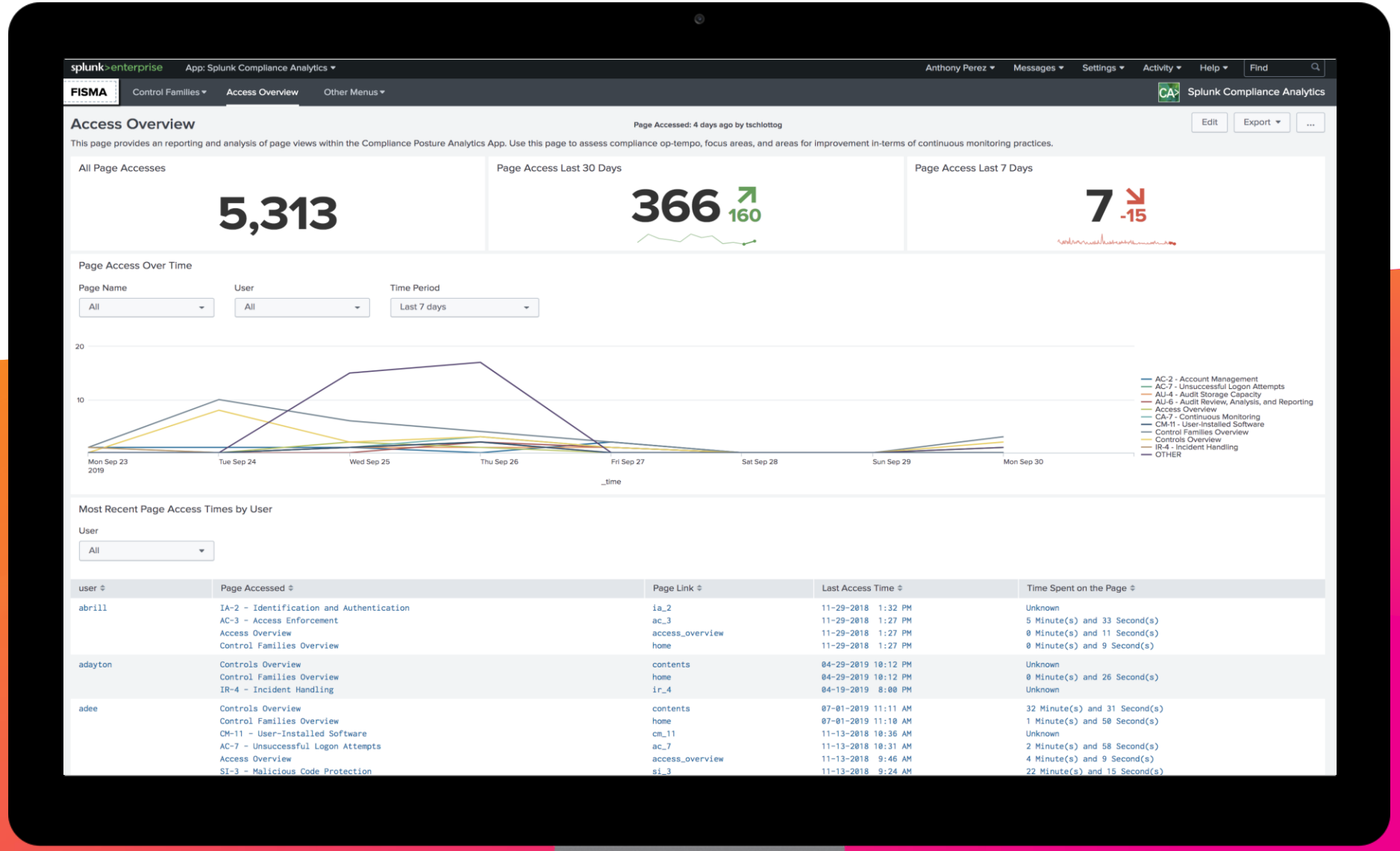
© 2019 SPLUNK INC.



Splunk Compliance Analytics

splunk> .conf19

© 2019 SPLUNK INC.



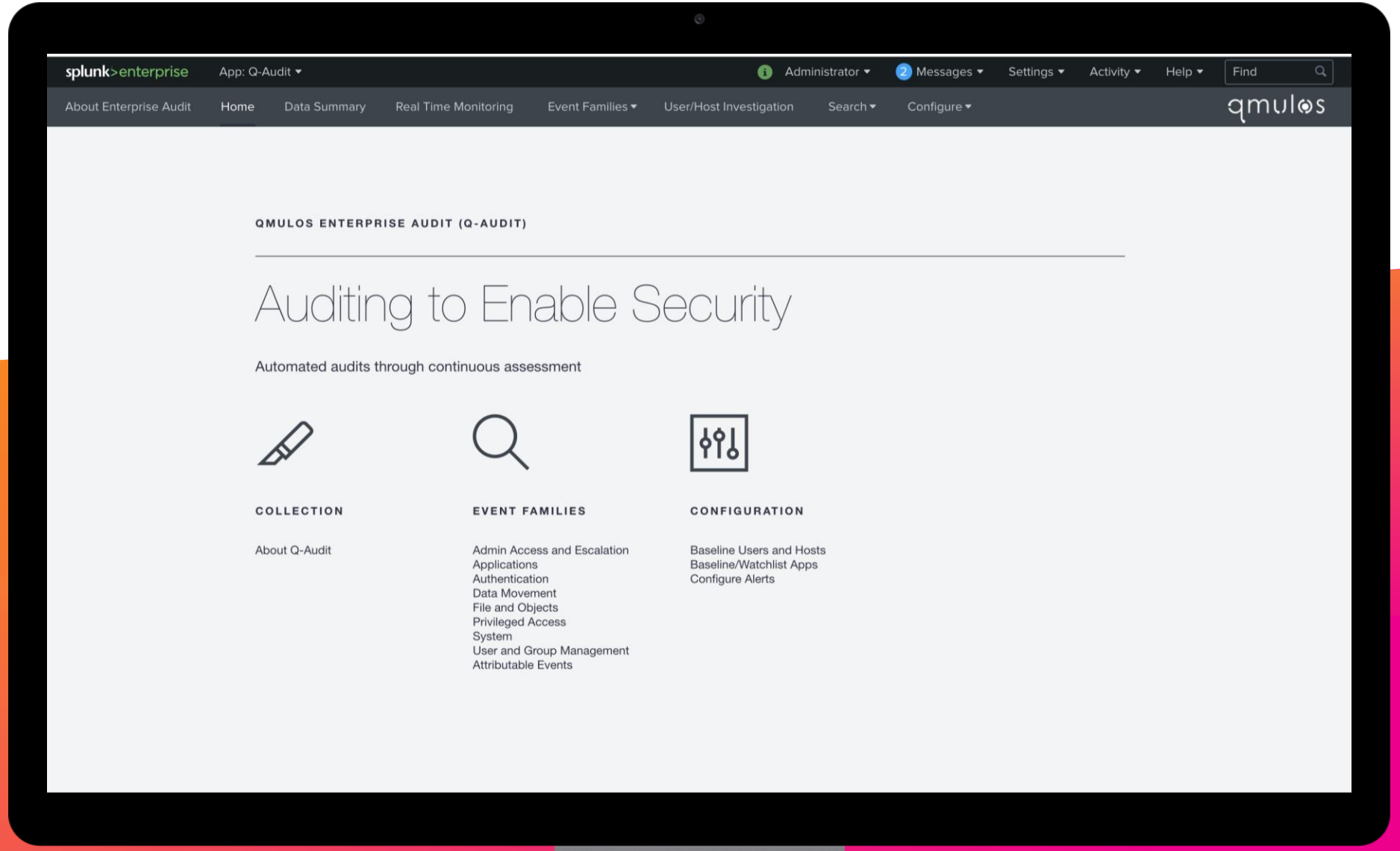
Splunk Compliance Analytics

splunk> .conf19

© 2019 SPLUNK INC.

Q-Audit

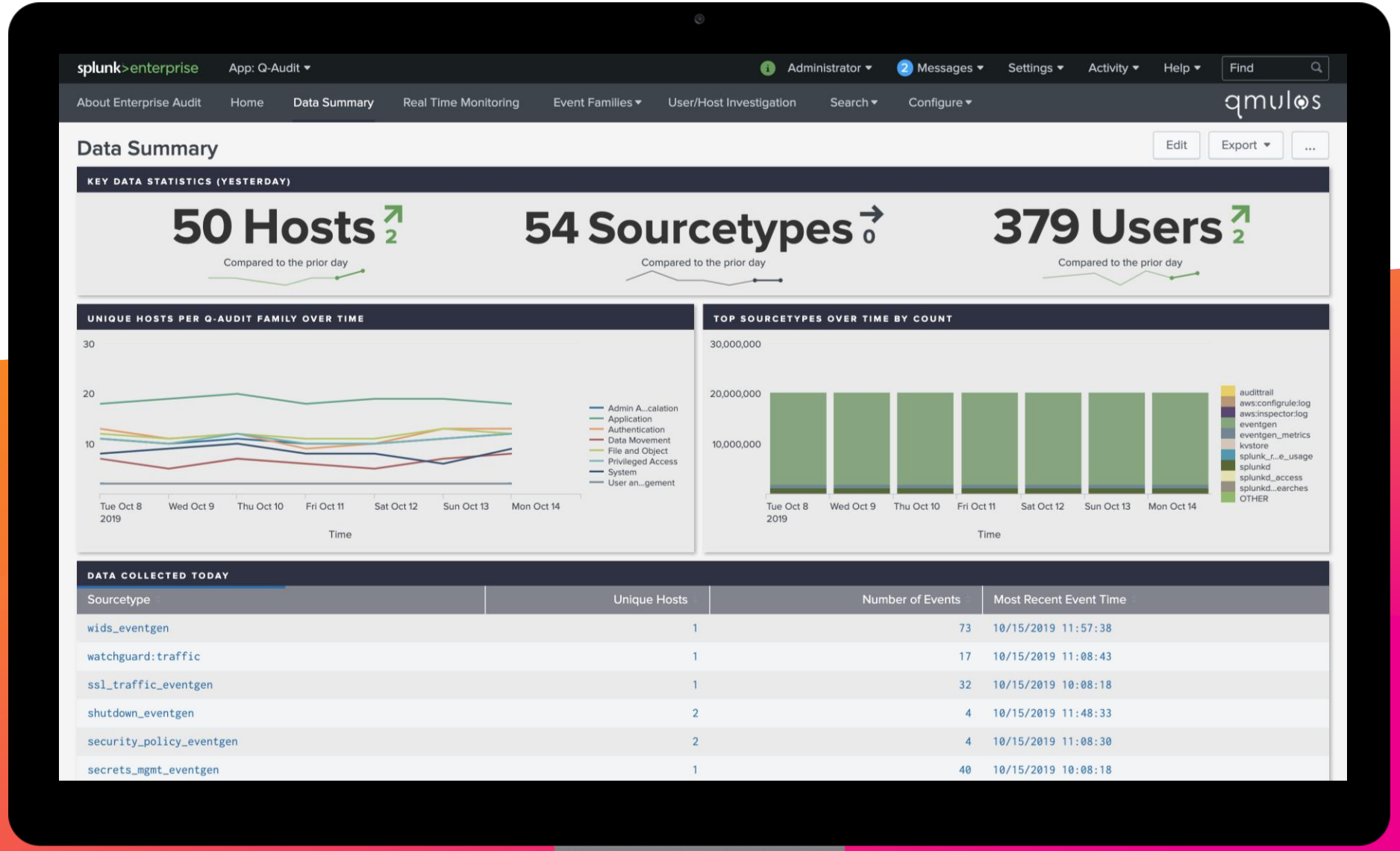
© 2019 SPLUNK INC.



Q-Audit

splunk> .conf19

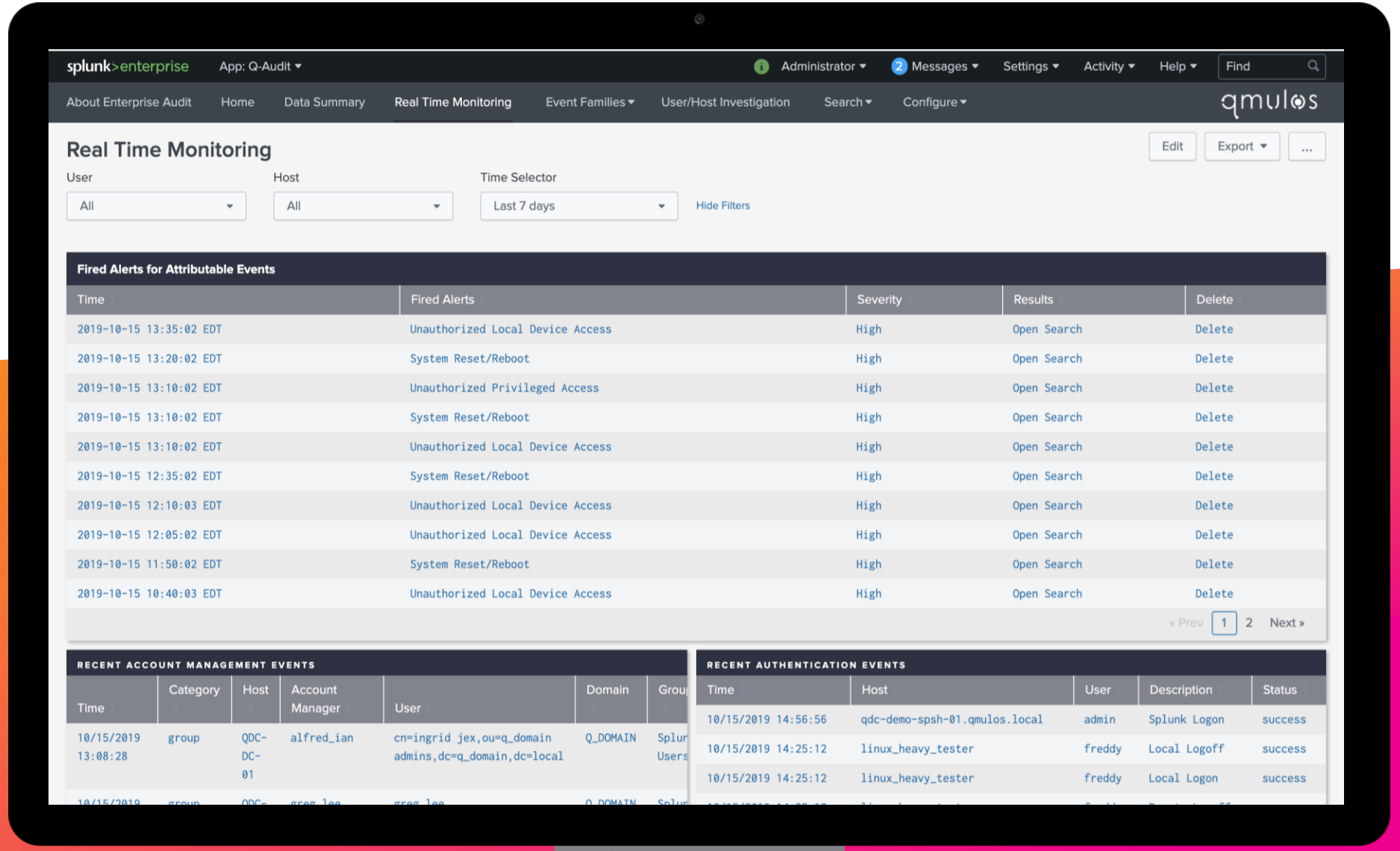
© 2019 SPLUNK INC.



Q-Audit

splunk> .conf19

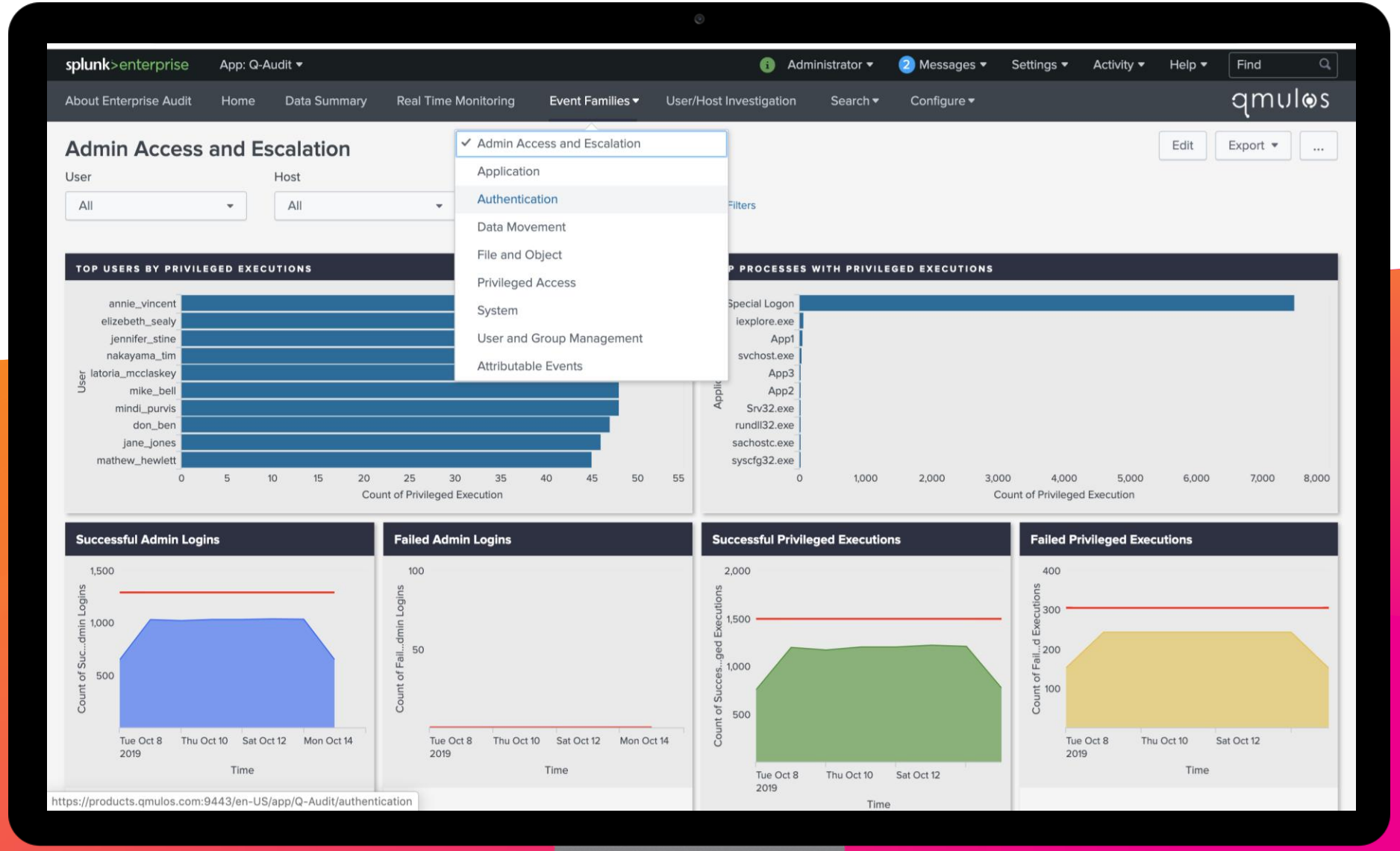
© 2019 SPLUNK INC.



Q-Audit

splunk> .conf19

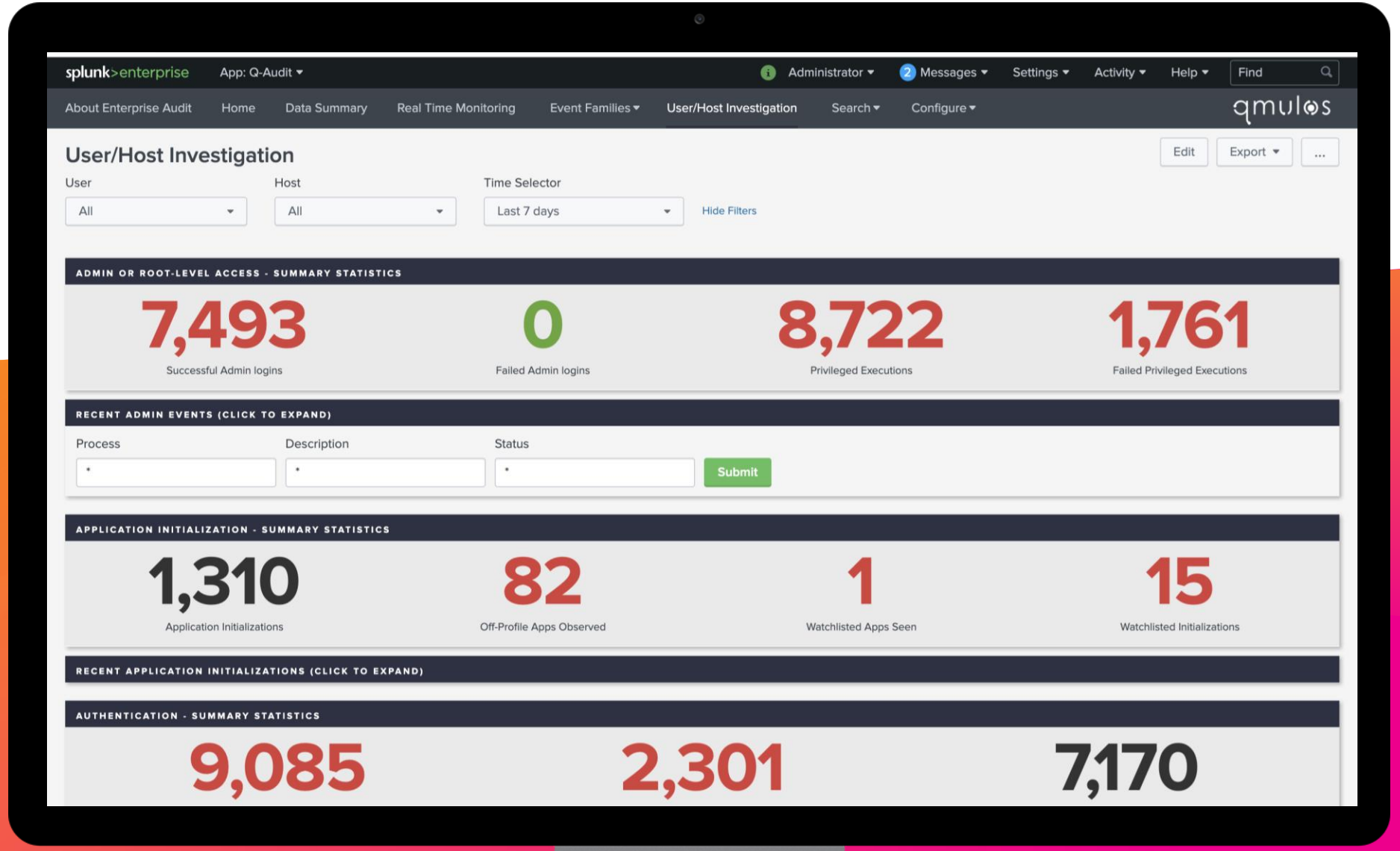
© 2019 SPLUNK INC.



Q-Audit

splunk> .conf19

© 2019 SPLUNK INC.



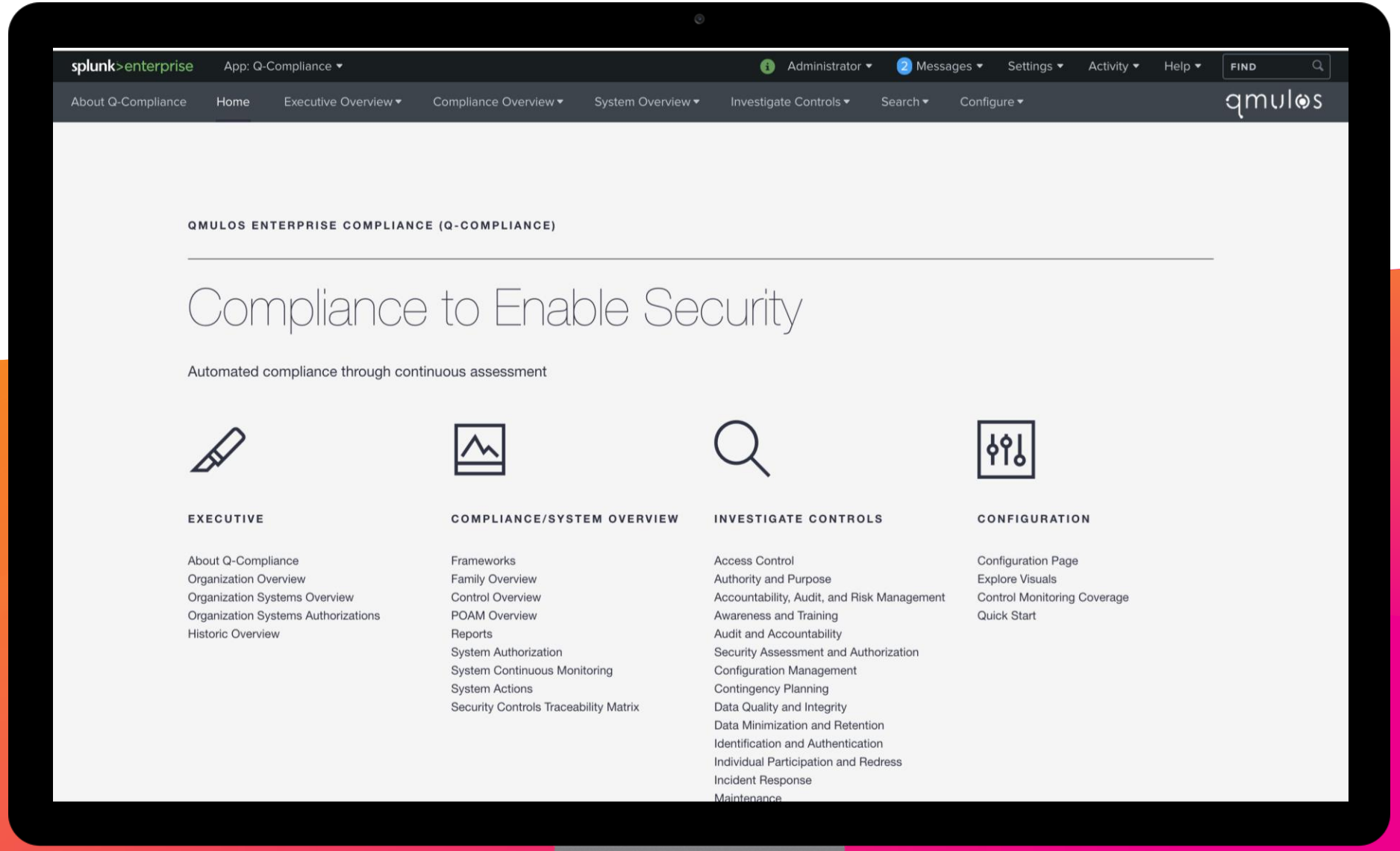
Q-Audit

splunk> .conf19

© 2019 SPLUNK INC.

Q-Compliance

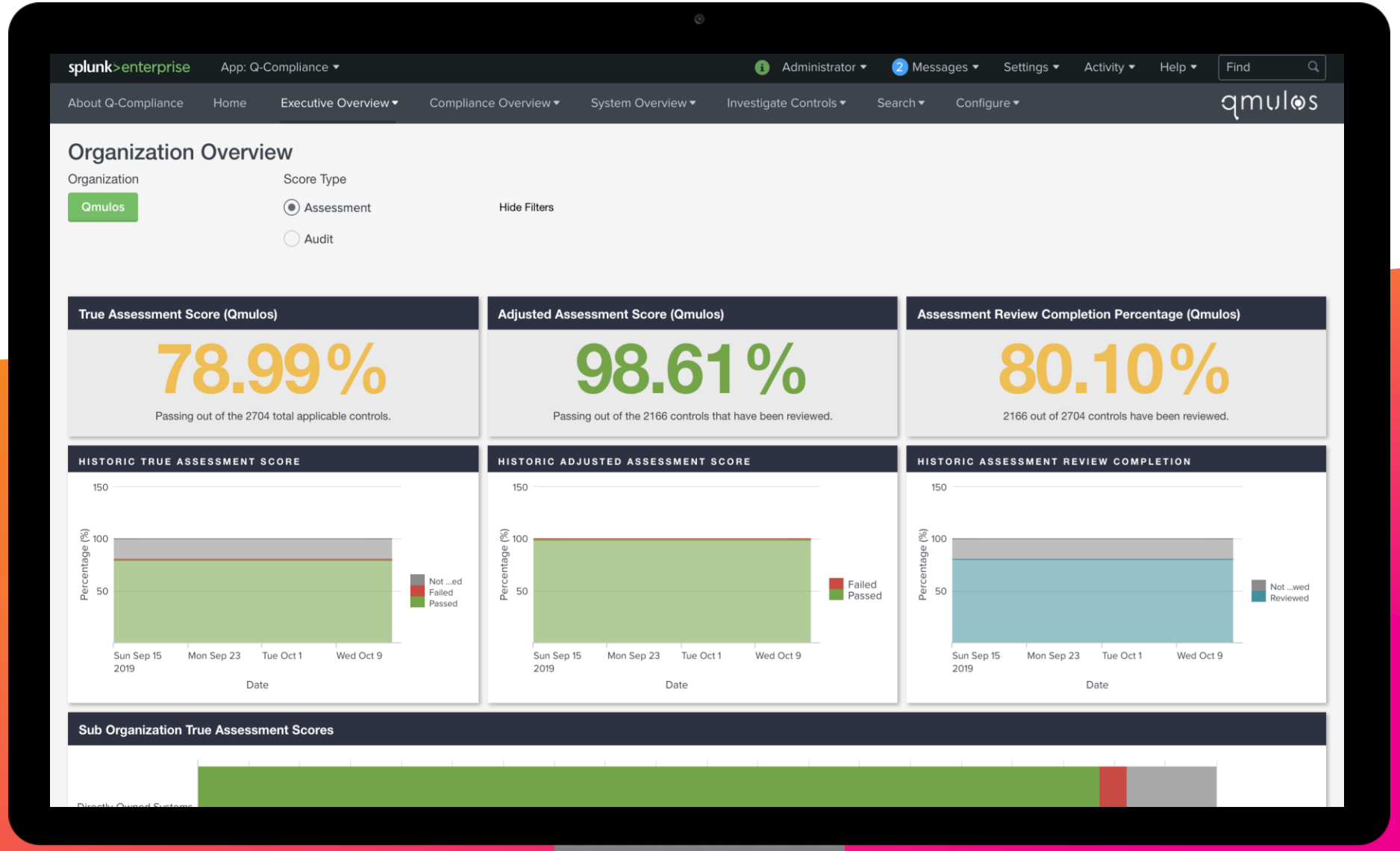
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

© 2019 SPLUNK INC.



Q-Compliance

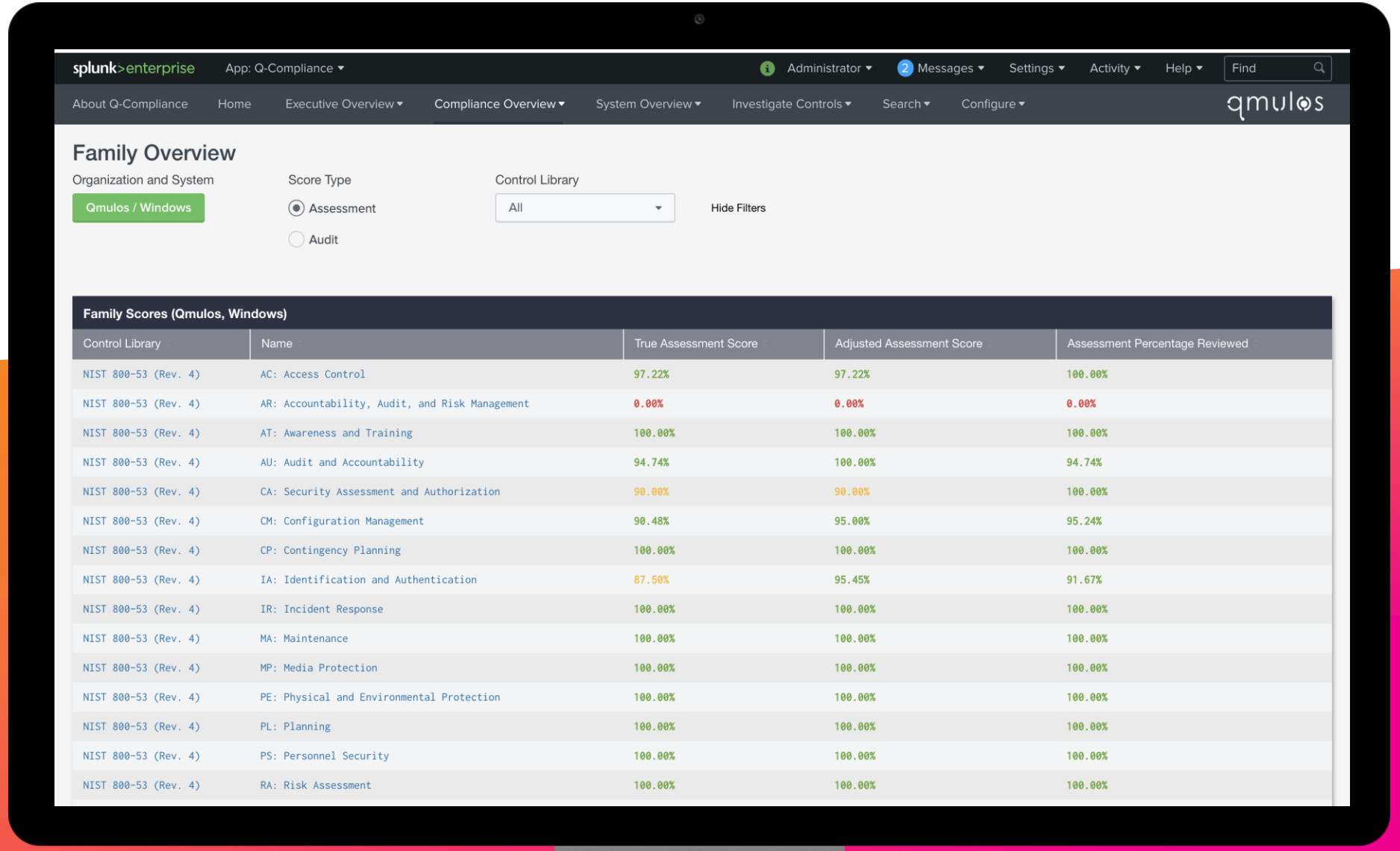
splunk> .conf19

© 2019 SPLUNK INC.

Q-Compliance

splunk> .conf19

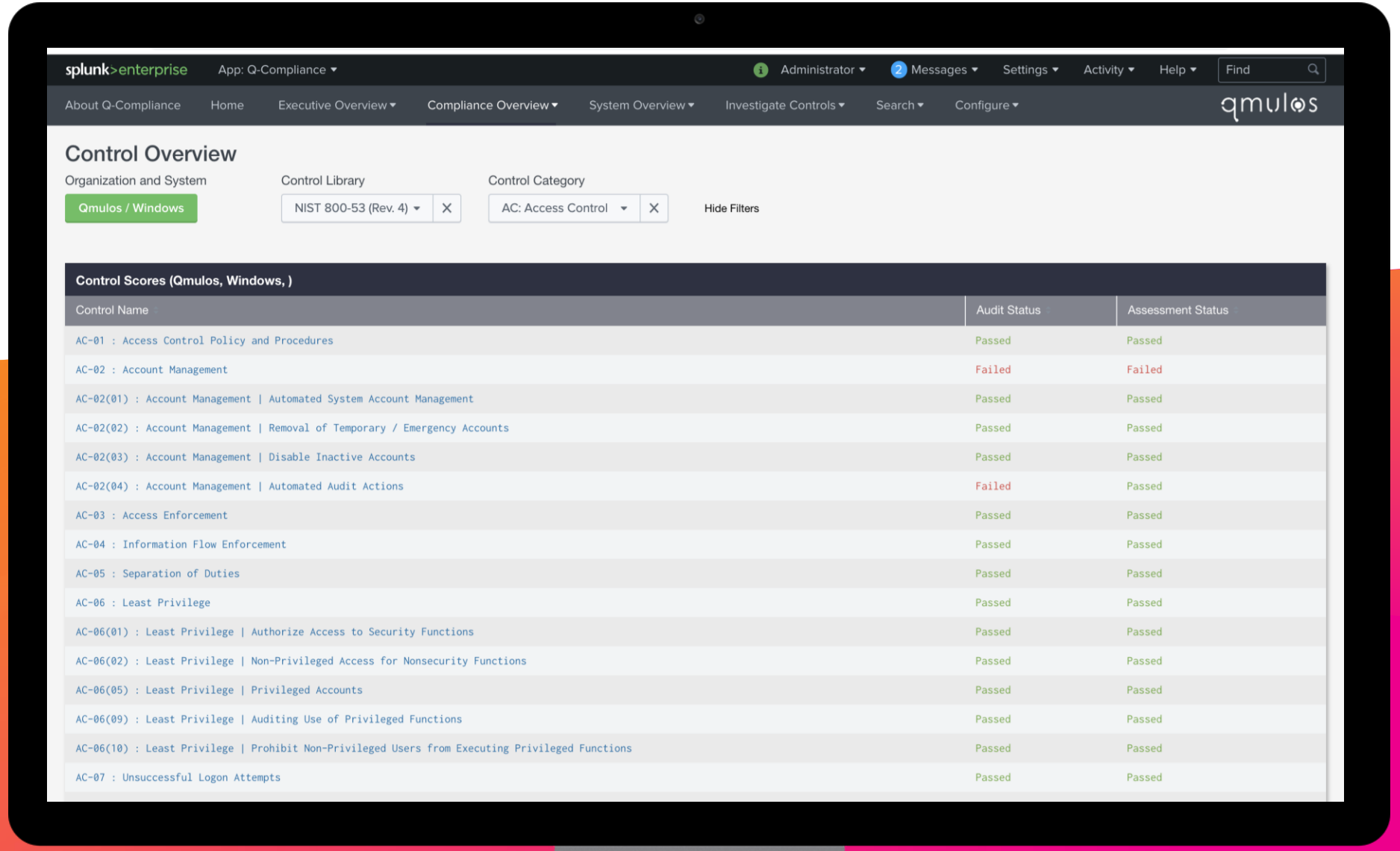
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

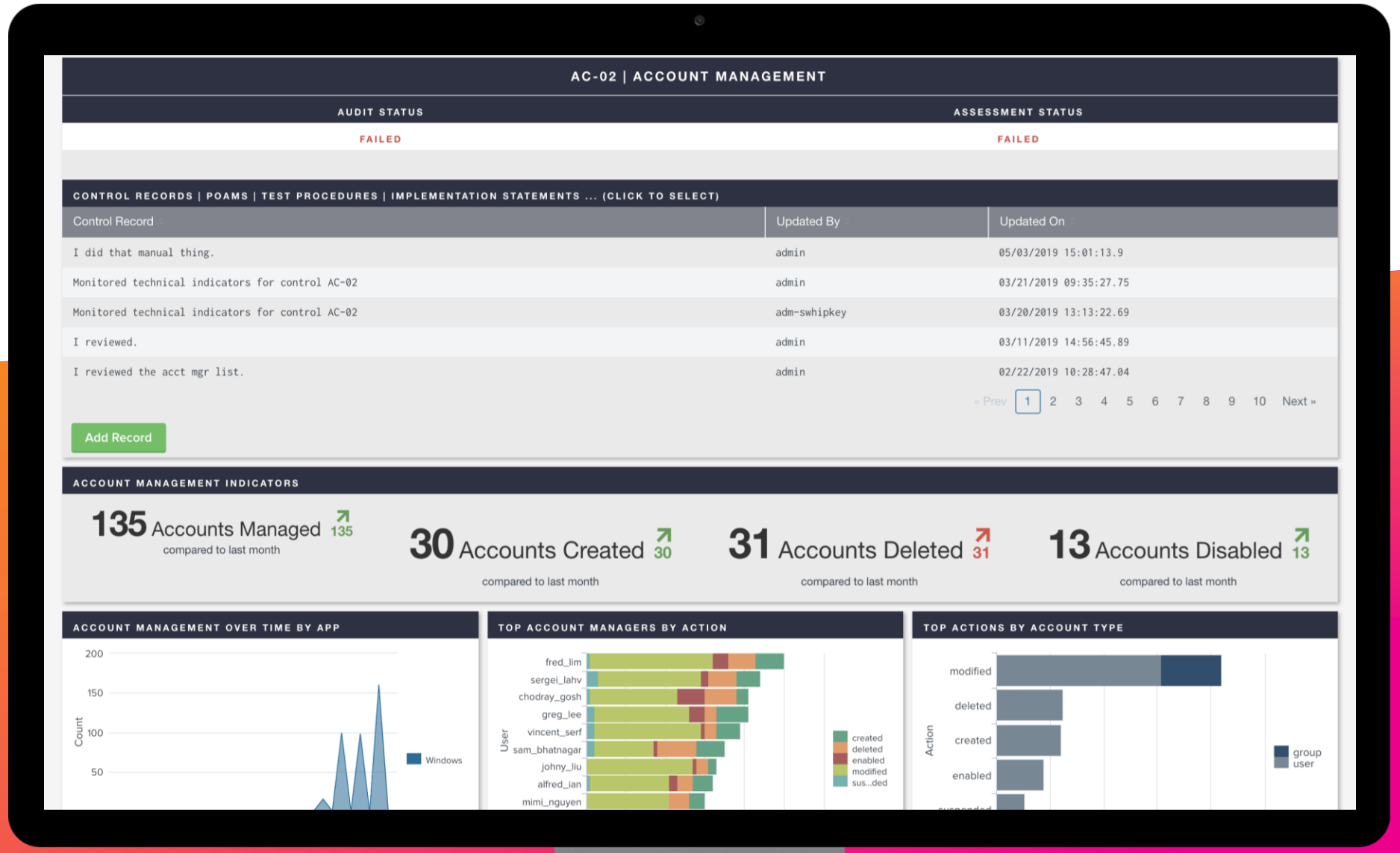
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

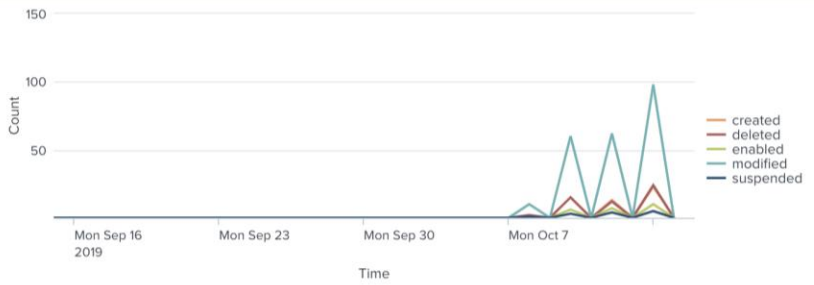
© 2019 SPLUNK INC.

« Prev 1 2 Next »

Add Record

ACCOUNT MANAGEMENT ACTIVITY BY ACTION

Click On Line for Detail View



ACCOUNT MANAGEMENT ACTIVITY BY STATUS

Click On Line for Detail View

SECURITY SCAN STATISTICS (CLICK ON STATS FOR ADDITIONAL DETAILS)

100.00%	0.00%	0.00%
Passing Results	Failing Results	Other Results

ASSIGNED EVIDENCE

File Name	Content Type	Content Size	Description	Assigned	Assigned By	Uploaded	Uploaded By
new screenshot	link	0	www.dos.gov	2018-07-12 10:25:46	admin	2018-07-12 10:25:46	admin

EVIDENCE MANAGEMENT

Select from existing evidence:

Previously uploaded evidence ▾ Assign

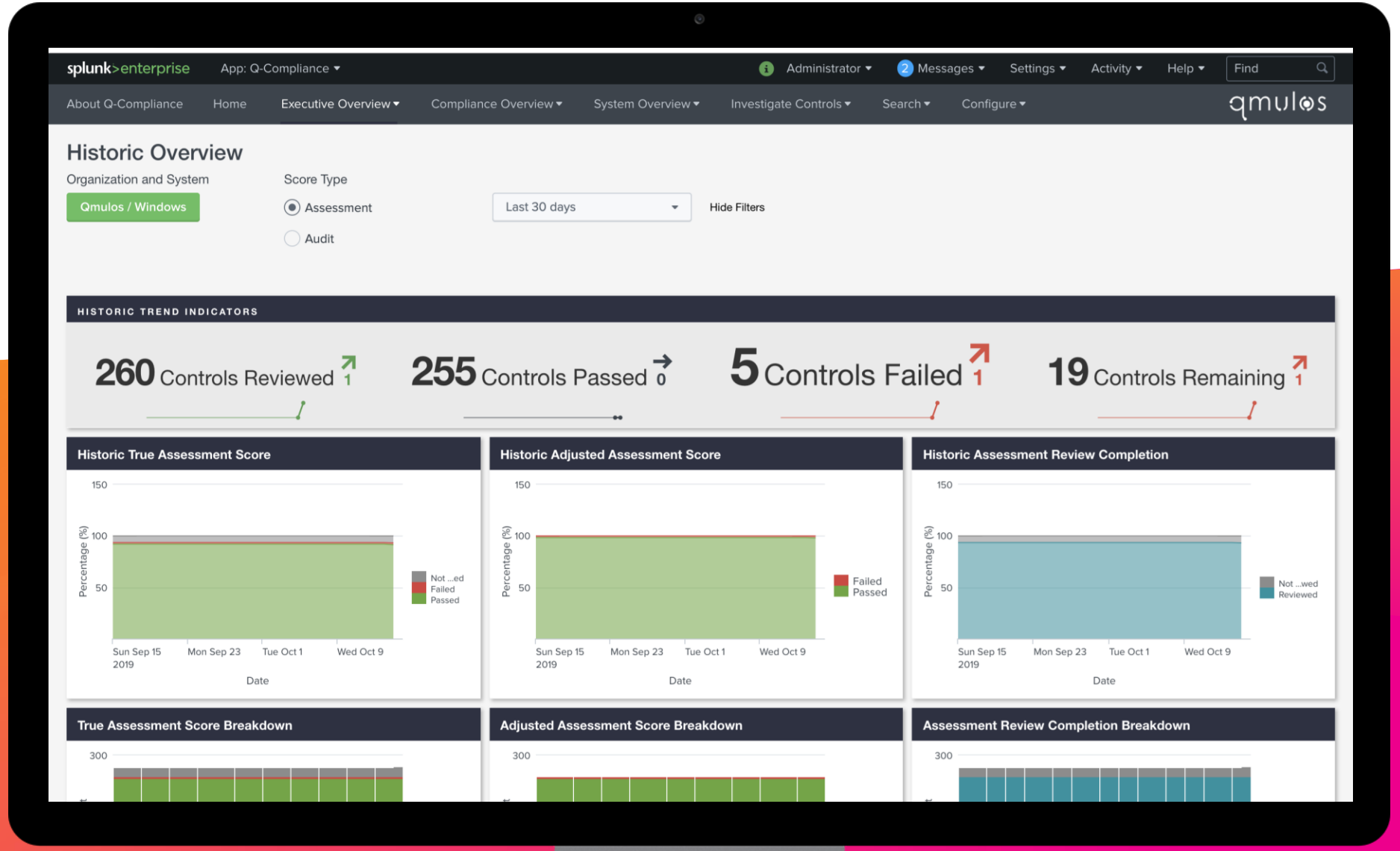
Upload new evidence:

Choose File No file chosen Upload Add Evidence Link

Q-Compliance

splunk> .conf19

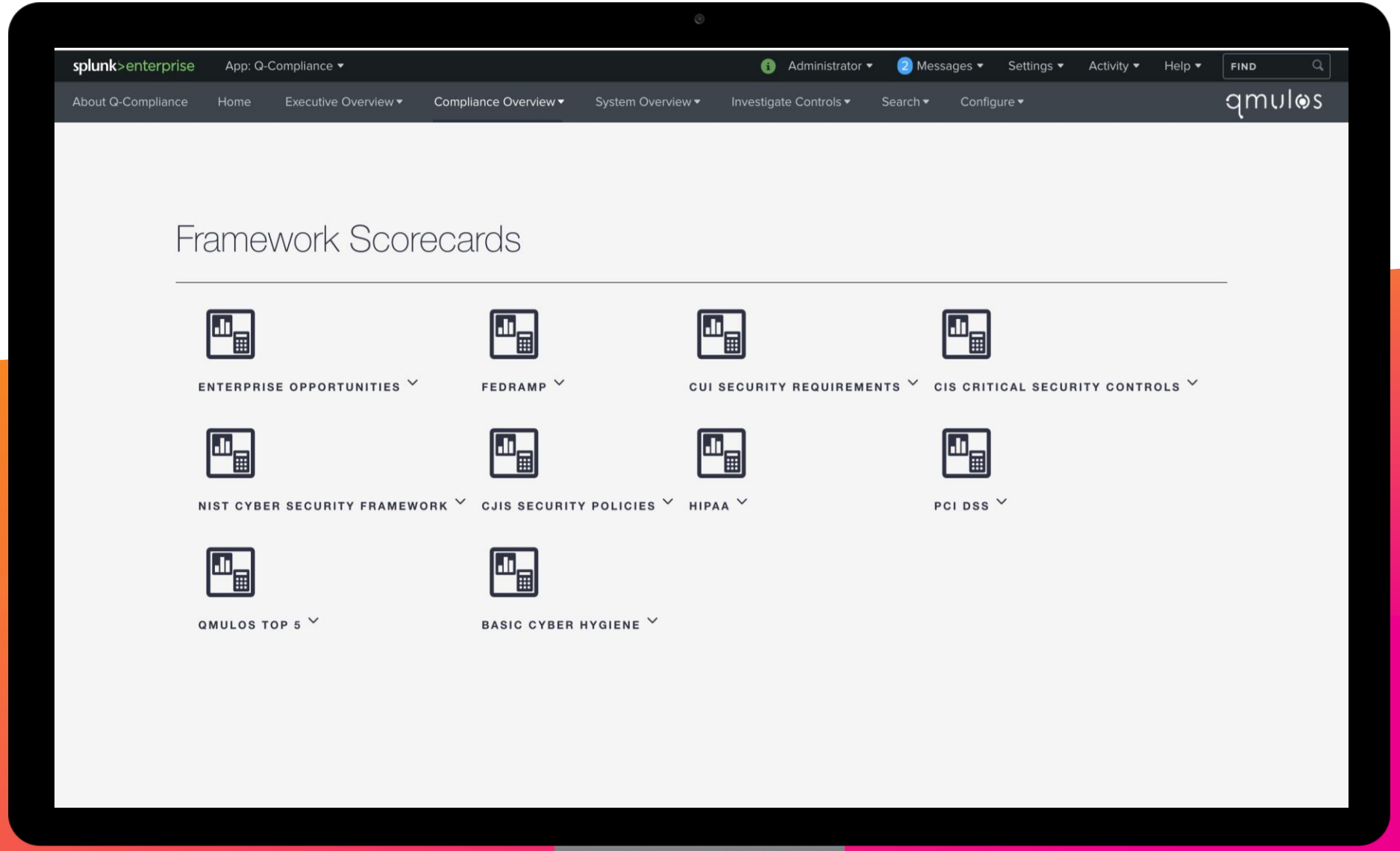
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

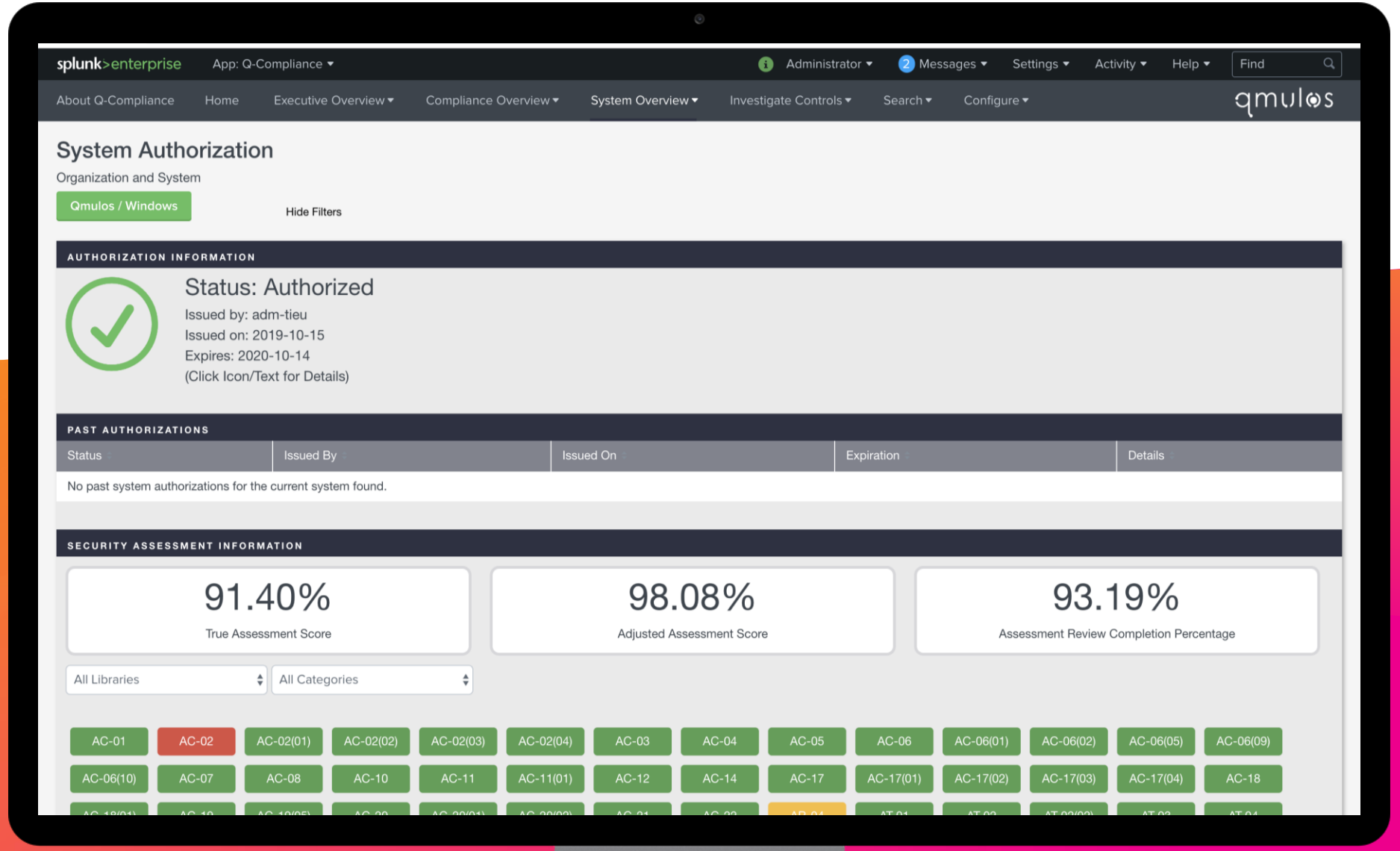
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

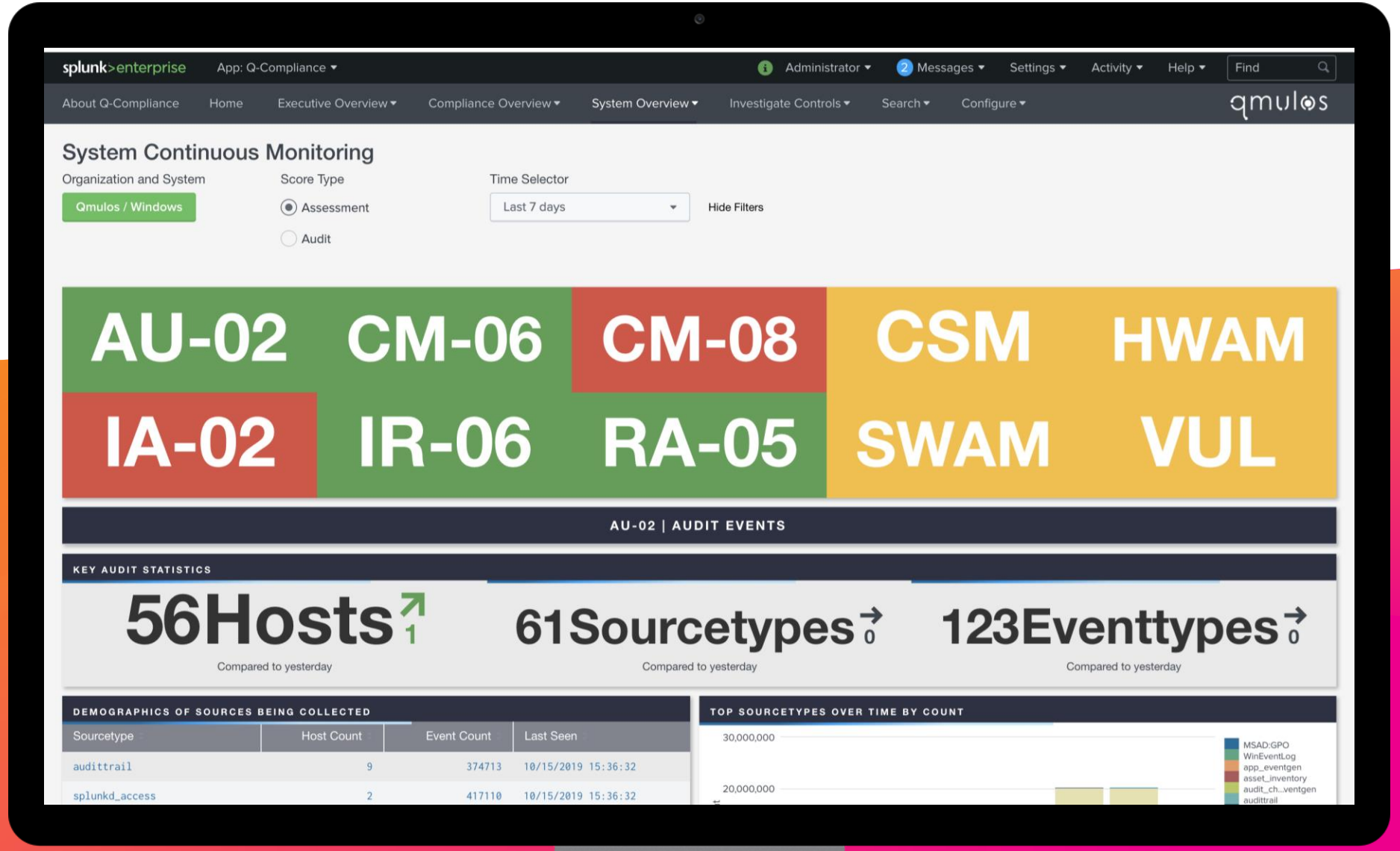
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

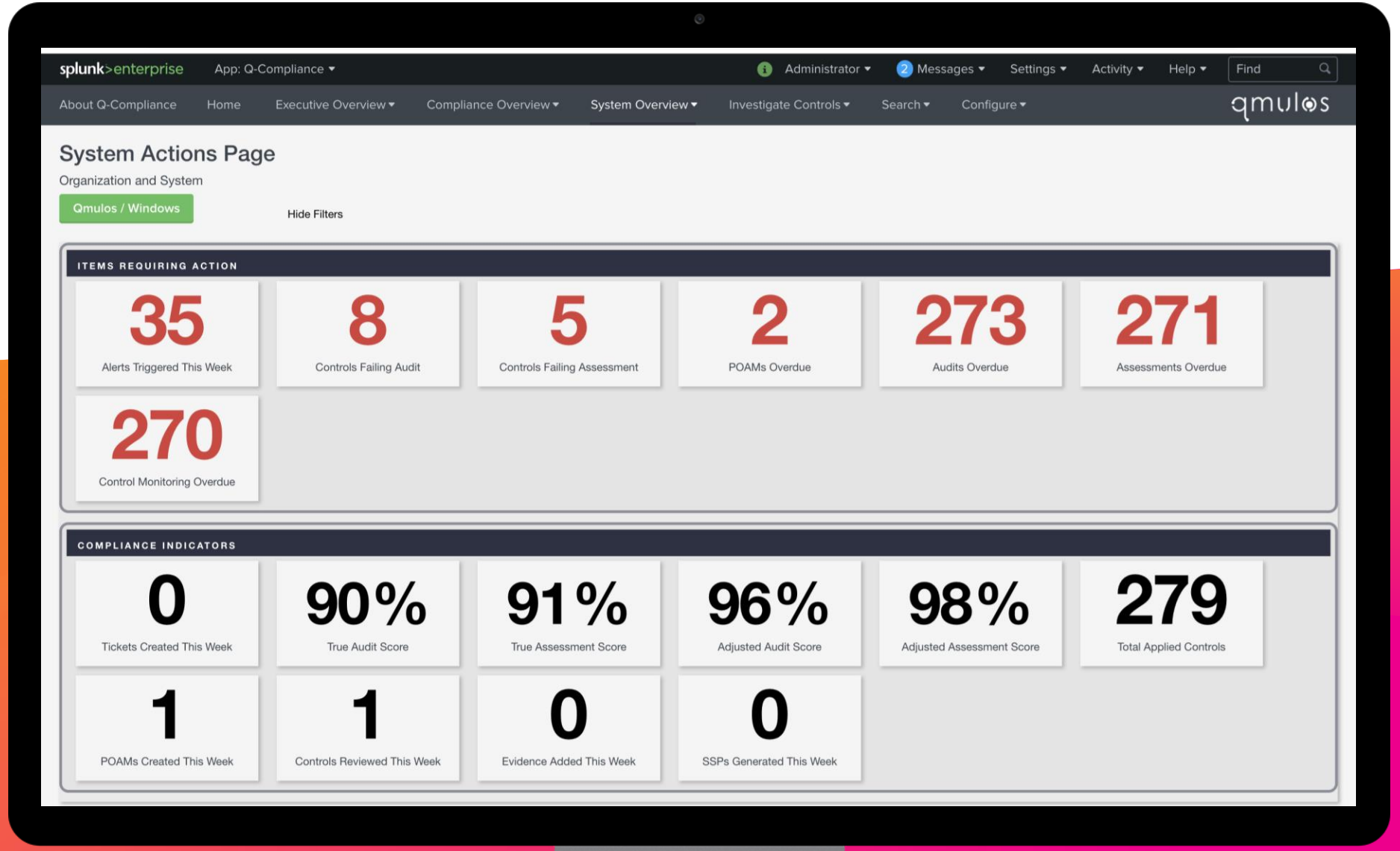
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

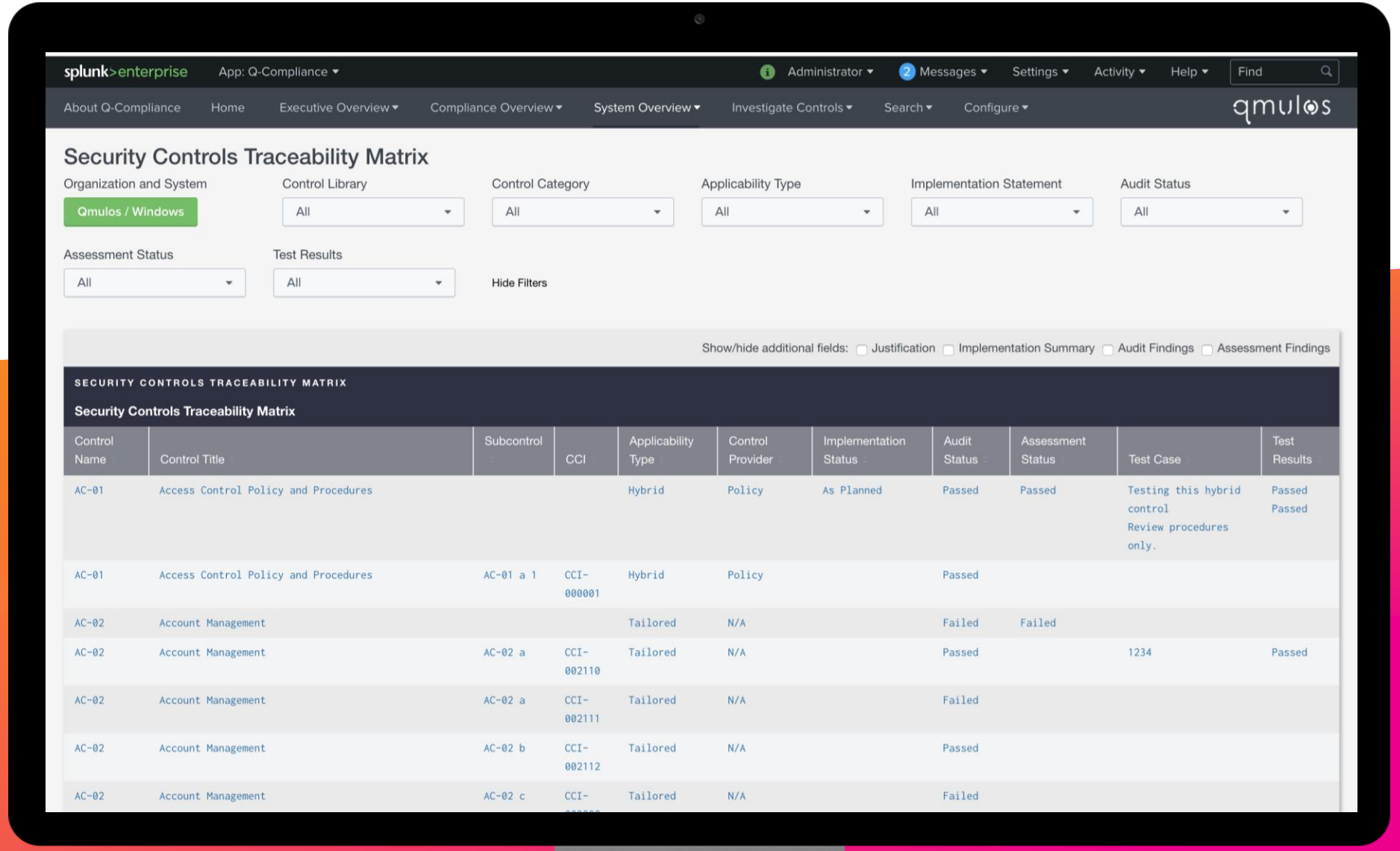
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

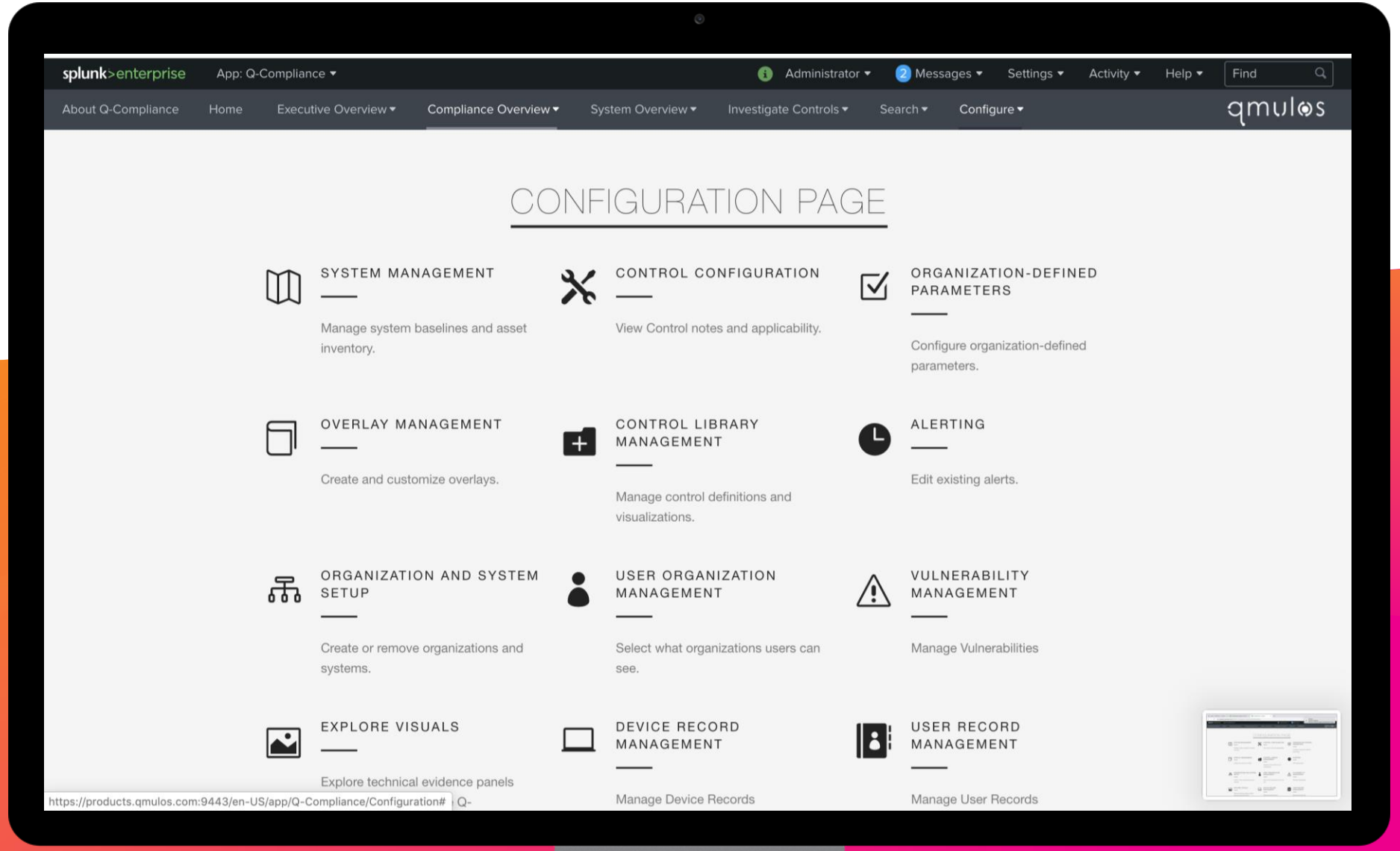
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

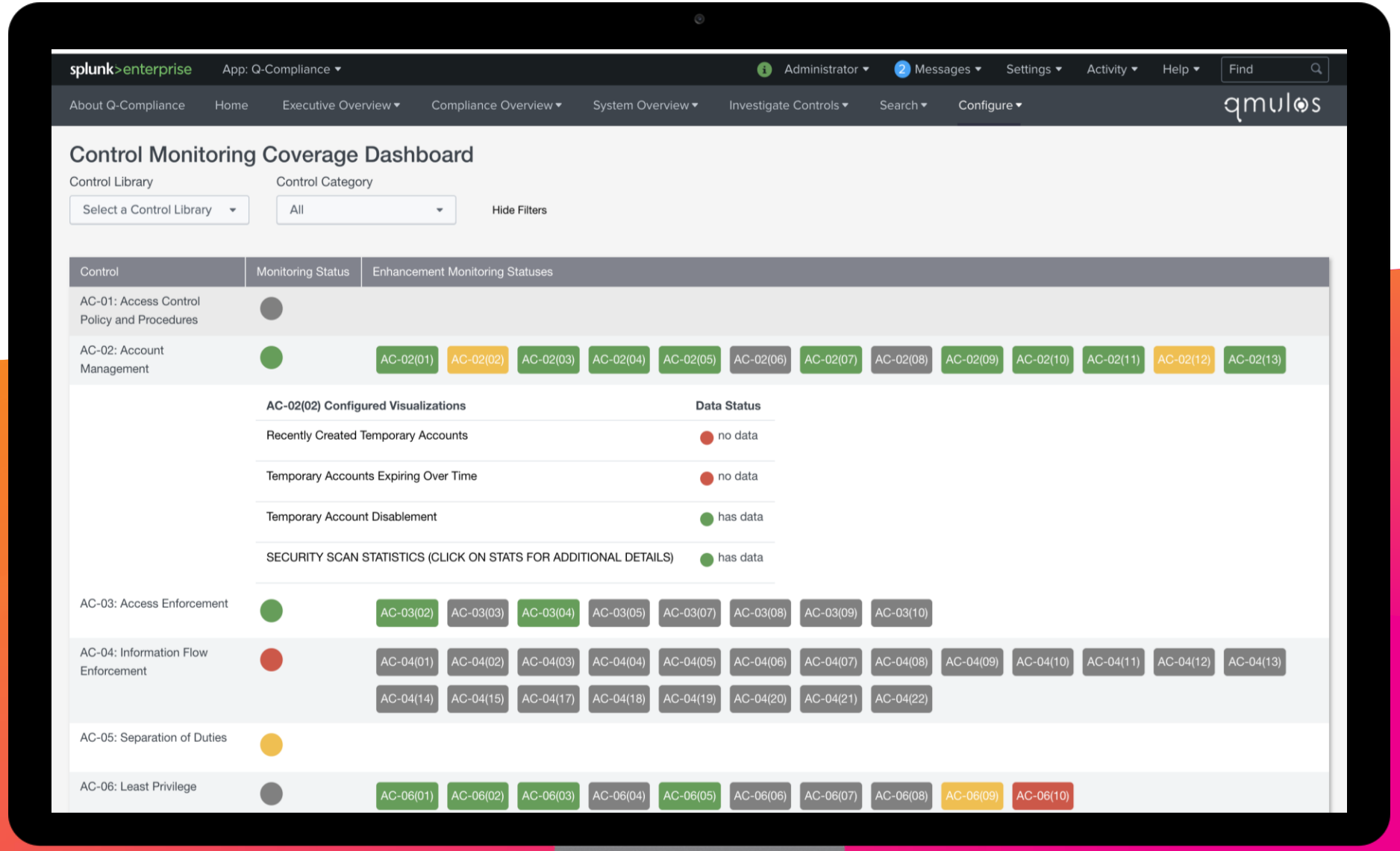
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

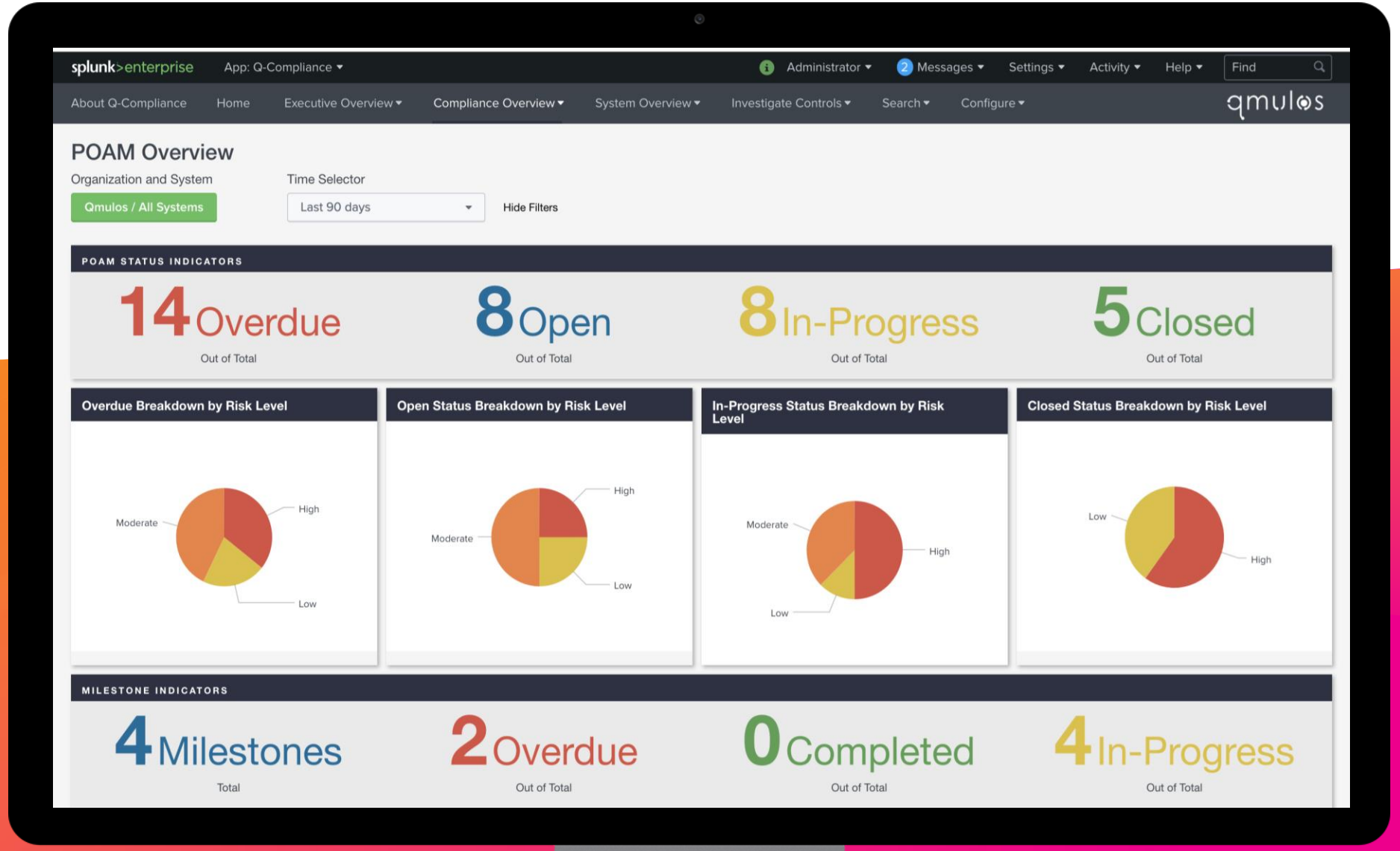
© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19

© 2019 SPLUNK INC.



Q-Compliance

splunk> .conf19