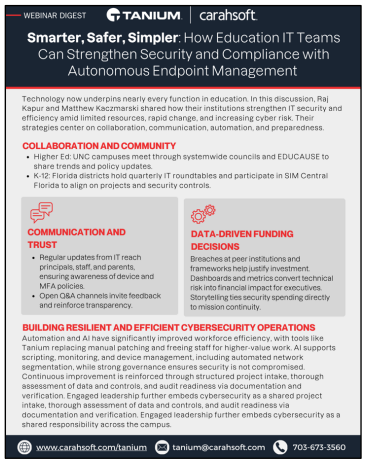
WEBINAR DIGEST TANIUM | carahsoft

Smarter, Safer, Simpler: How Education IT Teams Can Strengthen Security and Compliance with Autonomous Endpoint Management

Technology now underpins nearly every function in education. In this discussion, Raj Kapur and Matthew Kaczmarski shared how their institutions strengthen IT security and efficiency amid limited resources, rapid change, and increasing cyber risk. Their strategies center on collaboration, communication, automation, and preparedness.

COLLABORATION AND COMMUNITY

- Higher Ed: UNC campuses meet through systemwide councils and EDUCAUSE to share trends and policy updates.
- K-12: Florida districts hold quarterly IT roundtables and participate in SIM Central Florida to align on projects and security controls.

COMMUNICATION AND TRUST

- Regular updates from IT reach principals, staff, and parents, ensuring awareness of device and MFA policies.
- Open Q&A channels invite feedback and reinforce transparency.

DATA-DRIVEN FUNDING DECISIONS

Breaches at peer institutions and frameworks help justify investment. Dashboards and metrics convert technical risk into financial impact for executives. Storytelling ties security spending directly to mission continuity.

BUILDING RESILIENT AND EFFICIENT CYBERSECURITY OPERATIONS

Automation and AI have significantly improved workforce efficiency, with tools like Tanium replacing manual patching and freeing staff for higher-value work. AI supports scripting, monitoring, and device management, including automated network segmentation, while strong governance ensures security is not compromised. Continuous improvement is reinforced through structured project intake, thorough assessment of data and controls, and audit readiness via documentation and verification. Engaged leadership further embeds cybersecurity as a shared project intake, thorough assessment of data and controls, and audit readiness via documentation and verification. Engaged leadership further embeds cybersecurity as a shared responsibility across the campus.

www.carahsoft.com/tanium tanium@carahsoft.com 703-673-3560

Smarter, Safer, Simpler: How Education IT Teams Can Strengthen Security and Compliance with Autonomous Endpoint Management

Thank you for downloading this Tanium resource. Carahsoft is the official government distributor for Tanium cybersecurity solutions available via GSA, NASA SEWP V, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Tanium's solutions, please check out the following resources and information:

For additional resources:
carah.io/taniumresources

For upcoming events:
carah.io/taniumevents

For additional Tanium solutions:
carah.io/taniumsolutions

For additional cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
tanium@carahsoft.com

703-673-3560

To purchase, check out the contract vehicles available for procurement:
carah.io/taniumcontracts

For more information, contact Carahsoft or our reseller partners:
tanium@carahsoft.com | 703-673-3560

WEBINAR DIGEST

Smarter, Safer, Simpler: How Education IT Teams Can Strengthen Security and Compliance with Autonomous Endpoint Management

Technology now underpins nearly every function in education. In this discussion, Raj Kapur and Matthew Kaczmarski shared how their institutions strengthen IT security and efficiency amid limited resources, rapid change, and increasing cyber risk. Their strategies center on collaboration, communication, automation, and preparedness.

COLLABORATION AND COMMUNITY

- Higher Ed: UNC campuses meet through systemwide councils and EDUCAUSE to share trends and policy updates.
- K-12: Florida districts hold quarterly IT roundtables and participate in SIM Central Florida to align on projects and security controls.

COMMUNICATION AND TRUST

- Regular updates from IT reach principals, staff, and parents, ensuring awareness of device and MFA policies.
- Open Q&A channels invite feedback and reinforce transparency.

DATA-DRIVEN FUNDING DECISIONS

Breaches at peer institutions and frameworks help justify investment. Dashboards and metrics convert technical risk into financial impact for executives. Storytelling ties security spending directly to mission continuity.

BUILDING RESILIENT AND EFFICIENT CYBERSECURITY OPERATIONS

Automation and AI have significantly improved workforce efficiency, with tools like Tanium replacing manual patching and freeing staff for higher-value work. AI supports scripting, monitoring, and device management, including automated network segmentation, while strong governance ensures security is not compromised. Continuous improvement is reinforced through structured project intake, thorough assessment of data and controls, and audit readiness via documentation and verification. Engaged leadership further embeds cybersecurity as a shared project intake, thorough assessment of data and controls, and audit readiness via documentation and verification. Engaged leadership further embeds cybersecurity as a shared responsibility across the campus.