FORTINET

CHECKLIST

How to Achieve Highly Effective Cybersecurity in Community Colleges: 4 Requisite Capabilities

Community colleges face security challenges similar to large universities, but with some important differences. A recent survey of community college CIOs found that 78% have a difficult time retaining IT talent and 77% identify hiring qualified IT personnel as a top campus IT priority.[1] In addition, many two-year institutions struggle to obtain adequate funding and lack highly skilled IT professionals: 67% say that their funding has not recovered from budget cuts in recent years.[2]

Against this backdrop, IT teams in community colleges are under considerable pressure to protect sensitive personal information, provide secure access to diverse devices, and work within budgetary guidelines.

Here are 4 key criteria to look for in a complete security solution for community colleges:

☑ Integrated security solutions

The attack surface is rapidly expanding because of a geographically dispersed student population, multiple campuses, and the need for anytime, anywhere connectivity. Securing the community college network starts with a solution that features seamless integration for all security components and rapid detection and remediation of security events. Next-generation firewalls with threat-intelligence sharing are the heart of effective institutional security, providing a high level of security while maintaining network performance.

☑ Secure remote access

Mobile device proliferation and the advent of the Internet of Things (IoT) dramatically increase the number of possible entry points for attackers. IT teams need solutions that provide visibility and control for all devices attached to the network. Endpoint protection against malicious threats extends effective security to the individual device. Access management including two-factor and one-time password authentication add an additional layer of protection.

☑ Artificial intelligence and sandboxing

Advanced exploits penetrate perimeter defenses and move through the network to create havoc and steal valuable information. Therefore, community colleges need solutions with intent-based segmentation to limit lateral threat movement and sandboxing capabilities to isolate unknown threats. Top-tier security solutions use artificial intelligence (AI) and machine learning (ML) to extract actionable insights and facilitate post-breach forensics.

☑ Automated operations and response

Complexity of legacy systems and advanced threats inhibit staff productivity and lengthen time to resolution—issues that strain small IT staffs to the limit. To meet this challenge, community colleges need single-pane-of-glass management, zero-touch provisioning, and orchestrated, automated response to threats in real time. These capabilities meet the needs of lean teams by enhancing productivity and speeding threat mitigation.

Integration and Automation Are Must-haves for Community College Security Solutions

When it comes to community college cybersecurity, the whole must be greater than the sum of the parts, an outcome that can only be achieved through integration and automation. CIOs should place a high priority on solutions that reduce the attack surface through integrated visibility, provide secure access for mobile devices, stop advanced threats with AI-driven breach prevention, and reduce complexity through automated operations and orchestration. Such top-tier solutions deliver tangible benefits including lower total cost of ownership, reduced operating expenses, stronger security for remote and mobile devices, and faster breach detection and mitigation.

[1] "2019 Campus Computing: The 30th National Survey of Computing and Information Technology in American Higher Education," The Campus Computing Project, October 15, 2019.

[2] Ibid.

FORTINET®

www.fortinet.com

Copyright © 2019 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

November 27, 2019 11:21 AM

D:\Fortinet\Work\2019\November\112719\checklist-community-colleges

538603-0-0-EN