FORTINET

How the Right Solutions Can Secure a University Network

Table of Contents

FORTINET

Executive Overview

As universities allow students, faculty, staff, and other stakeholders to bring more of their own devices to campus, CIOs become responsible for safeguarding an increasingly diverse and complex network environment. Additionally, they are responsible for protecting the growing amount of user data and applications in the cloud. The faster the university's attack surface expands, the more critical it is to develop an evolved network security strategy.

To protect their diverse applications and data assets, universities need to harness a suite of security solutions, including access and identity management, network access control, firewalls with advanced segmentation capabilities, and behavior analytics. Additionally, if the university intends to use software-defined wide-area networking (SD-WAN) to connect different campus locations, the SD-WAN edge solutions should have advanced security built in. Effective management of university network security requires solutions that are both powerful and tightly integrated for end-to-end coverage. Selecting the right solutions enables the university to provide a secure open network while protecting a wide variety of users, devices, applications, and data.

Introduction: Universities' Expanding Attack Surface Creates Security Risks

Bring-your-own-device (BYOD) policies are driving the expansion of the network attack surface at many universities. It is not uncommon for faculty to use personal devices to support learning and research activities. Meanwhile, students expect fast and seamless network connectivity for a wide array of mobile phones, tablets, gaming consoles, smart speakers, and more.[1] They may arrive on campus with eight or nine different devices,[2] with the expectation that each will have wireless internet access from anywhere on campus.

University CIOs are under pressure to meet these expectations. Pervasive and high-speed Wi-Fi may even be a differentiator in some students' college-selection process.[3]

However, each new device that connects to the university network presents a potential access point for attackers. Universities store a great deal of valuable data, from personally identifiable information (PII) on employees and students to research data in a wide range of scientific, medical, and military specialties. The existence of this data makes universities a key target for many cyber criminals.[4] Universities face the ongoing risk that providing access to a large number of third-party devices will expose new security gaps that attackers can compromise.

CIOs at large universities must ensure that their network is properly protected. Here are seven considerations for designing a security architecture that can thwart cyber criminals even as the university's attack surface continues to expand.

27

institutes of higher education in the United States, Canada, and Southeast Asia were attacked recently by nation-state hackers looking for military secrets.[5]

Efficiency Is Key in Identity and Access Management

Identity and access management solutions confirm the identity of each user and device as it enters the network. When considering their options, universities should look for products that automate these processes. With thousands of unique devices connecting each day, and a persistent shortage of cybersecurity skills, university IT team members cannot be expected to manually monitor and manage user and device access. Automation improves both the accuracy and the efficiency of these tasks. Best-in-class automated identity and access management solutions offer highly configurable automation settings, which enable security teams to select which tasks and events are handled automatically and which trigger alerts for human intervention.

Large universities should also look for an identity and access management solution that consolidates authentication services in one place—including sign-on services, certificate management, and guest management.

Solutions that combine automation and single-pane-of-glass management make it possible to oversee the entire authentication process from one central console. For universities with lean IT security teams, such a solution enables staff to maintain control of network access even as the number and diversity of devices continue to skyrocket.

Approximately 79% of organizations are opting into security automation.[6]

Network Access Control Is Necessary for Securing IoT Devices

The number of Internet-of-Things (IoT) devices on university campuses continues to multiply. Many schools are leveraging systems that automate lighting, air conditioning, parking alerts, and other areas of operations. The challenge for the CIO is that most IoT devices are innately insecure. They are intentionally designed to be as lightweight as possible, which means built-in security is minimal. In addition to BYOD policies, IoT devices create another potential avenue for attackers to use for access to the university network.

Universities that leverage IoT devices and systems are increasingly deploying network access control solutions to safely accommodate their IoT devices' network connections. As CIOs consider their options for network access control solutions, they need to make sure the solutions on their shortlist meet three key criteria:

- Provide comprehensive visibility into every device and user as they join the network.
- Appropriately limit where devices can go on the network.
- Include automated threat response so that the university can react to perceived threats within seconds.

"In two short years, there could be nearly 30 billion autonomous Internet-of-Things devices on [university] networks."[7]

Segmentation Can Mitigate Damage in the Event of a Breach

University security teams frequently use network segmentation to limit the size of their attack surface. Traditional segmentation involves dividing the network into sections that are separated by internal firewalls. If an attacker successfully accesses one network segment, this approach helps prevent lateral movement by which the attacker might access other crucial university data stores.

The effectiveness of traditional segmentation is limited, however, by its reliance on static trust valuations. The trustworthiness of devices and users may change both rapidly and frequently, especially in the event of a breach. Using static information to determine which assets can access each network segment undermines the effectiveness of the approach, especially on a network that provides access to thousands of devices every day.

Modern universities need a network security segmentation solution that provides dynamic trust valuations. The university's security team can build business rules that specify criteria for access to particular network resources. The solution then regularly and automatically reevaluates the trustworthiness of each user or device, based on the customized business rules. Trust valuations are always up to date, greatly improving the effectiveness of segmentation processes.

“Trust is not absolute, binary, or static. … the level of trust is dynamic and changes over time. Thus, access to the capabilities should be adapted.”[8]

SD-WAN Increases Performance but Raises Security Concerns

Universities that operate on multiple campuses need to provide efficient, secure connectivity between sites. Traditional WANs connect university campuses using multiprotocol label switching (MPLS) links. By contrast, SD-WAN solutions, which utilize public broadband, are both higher-bandwidth and more cost-effective. They replace the MPLS hub-and-spoke architecture with a direct internet connection in each location. This eliminates performance bottlenecks and significantly reduces costs.

However, SD-WAN technologies may also introduce security gaps. Because network traffic is no longer routed through the university data center as with a traditional WAN, it bypasses firewalls and security policies. This means SD-WAN solutions need to secure traffic themselves, but many come up short in this area. They may offer a basic layer of protection, but few SD-WAN solutions include built-in intrusion prevention system (IPS) technology, web filtering, or secure sockets layer (SSL)/transport layer security (TLS) inspection.

University CIOs considering SD-WAN for its cost and performance benefits must also ensure the solution they select can safeguard critical network communications. Secure SD-WAN solutions include deep packet inspection (SSL/TLS) and IPS, at minimum. They can also integrate with network threat intelligence to incorporate real-time information about emerging threats.

"The emergence of SD-WAN technology has been one of the fastest industry transformations we have seen in years. Organizations of all sizes are modernizing their wide-area networks to provide improved user experience for a range of cloud-enabled applications."[9]
– Rohit Mehra, VP, Network Infrastructure, IDC

Cloud Security Requires Special Consideration

Universities are increasingly leveraging cloud-based learning tools and data storage. Whether they utilize private clouds, public clouds, Software-as-a-Service (SaaS) solutions, or a hybrid cloud approach, universities are fully responsible for securing their own information. The cloud provider is responsible only for keeping its infrastructure and platforms functional.

Thus, university CIOs need to make cloud security a central element of their overall security strategy. They should look for a cloud security solution that offers:

- Native integration with each major cloud provider serving faculty, administrators, and students
- Automated management of the security infrastructure to streamline centralized oversight of diverse cloud solutions
- Broad, multilayered protection to secure every part of the evolving attack surface among multi-cloud environments

Whether they utilize private clouds, public clouds, Software-as-a-Service (SaaS) solutions, or a hybrid cloud approach, universities are fully responsible for securing their data.

User and Entity Behavior Analytics Protects Against Insider Threats

It is not pleasant to consider the frequency with which insiders perpetrate cyber crimes. For CIOs of large universities, however, this is an unavoidable truth. Studies routinely discover attacks are initiated from within, particularly by students who are either disgruntled or looking to give themselves an academic or other advantage. One recent study found that students are more likely than criminal hacking groups to attack university networks.[10]

The proliferation of insider threats raises the importance of securing the internal network through segmentation. It shows that security segmentation must not only be able to deter external hackers but also to prevent legitimate network users from accessing data they are not authorized to see.

Universities can further thwart inside attacks by layering a user and entity behavior analytics (UEBA) solution on top of segmentation policies. These solutions continuously monitor the activities of users and endpoints, looking for anomalies that might indicate nefarious intentions. When they detect suspicious behavior, they automatically alert security staff.

In an ideal world, all students, faculty, and staff would be entirely trustworthy. In the real world, however, the prudent CIO deploys this extra layer of protection and visibility over the university network.

$8.76M

—the average cost of an insider threat in 2018.[11]

Integrated Security Speeds Response, Bridges Skills Gap

Like any organization facing significant threats, a large university needs a comprehensive approach to network security. Selecting solutions that integrate tightly strengthens the institution's ability to respond to threats in a coordinated manner.

Consider a security infrastructure that consists of myriad point solutions. A threat detected in one area may still be able to penetrate other network defenses. However, when a university deploys a suite of solutions that comprise a network-wide security fabric, those solutions can exchange information on detected threats and respond faster in a coordinated way. To the extent that information exchange is automated, the speed of response will approach real time, and will also be more accurate.

In any case, an integrated security infrastructure can provide a single IT security team member complete visibility into threat protection across the university's network, including all satellite campuses and public clouds in which the university runs its applications. Thus, even a minimally staffed IT department can maintain competent threat protection for the university's expanding range of technology services.

When a university deploys a suite of solutions that integrate into a networkwide security fabric, those solutions can communicate about detected threats and respond in a coordinated way.

Conclusion: How to Achieve Best-of-Breed Security

As a university's attack surface expands, its approach to network security must evolve to keep critical research, PII, and other data secure. The CIO must evaluate several types of solutions, including, but not limited to, next-generation firewalls (NGFWs) for the campus and the cloud, identity and access management, SD-WAN technologies, and behavior analytics.

Each of these solutions must be among the best in its class in terms of its ability to prevent attacks—and to do so with minimal impact on network performance. If enabling advanced features such as IPS creates latency for network traffic, security staff will be tempted to turn them off, undermining network security and defeating the purpose of the solution.

In addition to considering the features and capabilities of each prospective product, the solution research process must involve evaluations of whether integration among the various products facilitates a coordinated, networkwide response—or whether a failure to integrate might leave areas of the network vulnerable. Moreover, if the university is grappling with the common strain of lean IT staffing, manageability of the overall security infrastructure needs to be a key consideration.

Securing the network of a large university is undoubtedly challenging. A holistic solution research process will help ensure that the CIO gets the right products in the right places to effectively protect all of the university's highly valuable data, applications, users, and devices.

[1] Lindsay McKenzie, "At What Cost Wi-Fi?," Inside Higher Ed, April 17, 2018.

[2] Ibid.

[3] "Ohio State University trustees approve contract with Apple to launch Digital Flagship initiative," Ohio State News, April 6, 2018.

[4] "Strategies for Research Cybersecurity and Compliance from the Lab," Internet2 Global Summit, March 8, 2019.

[5] Lindsay McKenzie, "On Red Alert," Inside Higher Ed, March 6, 2019.

[6] Ericka Chickowski, "The Cybersecurity Automation Paradox," Dark Reading, April 18, 2019.

[7] Eli Zimmerman, "How Universities Can Mitigate IoT Risk on Campus," EdTech, January 15, 2019.

[8] Neil MacDonald, "Zero Trust Is an Initial Step on the Roadmap to CARTA," Gartner, December 10, 2018.

[9] "SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022," IDC, August 7, 2018.

[10] Naveen Goud, "Students are responsible for cyber attacks on Universities and Colleges," Cybersecurity Insiders, accessed September 3, 2019.

[11] "2018 Cost of Insider Threats: Global Organizations," Ponemon Institute, April 2018.

www.fortinet.com

410893-0-0-EN

September 7, 2019 11:16 PM

eb-right-solutions-secure-university