

Scenario

Even before the pandemic, endpoint security had begun to feel unmanageable at many colleges and universities. Andrea Chen often found herself commiserating with fellow chief information security officers (CISOs) at other institutions about the difficulties arising from the proliferation of devices that students connect to campus networks, along with the relentless growth in the type and number of cyberattacks. Faculty and staff were also frequent targets of cyberattacks, and despite the benefits Chen had seen from an ongoing, campus-wide security awareness program, some users continued to be duped, costing her staff and the college rising sums of time and money to address.

When students left campus because of the pandemic, the college faced an even thornier security landscape, as users began logging in to institutional IT services from countless external networks, using countless more devices. The college's aging and outdated endpoint security solution, which consisted largely of antivirus/antimalware tools designed for a residential student body, was clearly not up to the task.

An exceptionally insidious attack at a peer institution gave Chen an opening to again make the case for new endpoint security measures. She had made similar pitches in the past, but institutional leaders balked at the price and complexity of the endpoint detection and response (EDR) approach she was proposing. This time, however, was different. Senior leaders at her college had seen—in the national news—the fallout from the hack at the peer institution. Chen was able to explain that an EDR solution could have prevented most of the damage that attack had caused because EDR can often spot suspicious behavior even before systems are compromised. If an attack does get through, EDR tools can interrupt it and keep it from spreading. An EDR approach would provide Chen and her staff with considerable visibility into what's happening on the college network, enabling them to continually adapt to emerging threats. Because an EDR system typically includes a cloud-based component that collects security data from a range of organizations, its machine learning is based on a broad set of parameters, increasing its effectiveness at identifying and responding to cyberattacks.

Officials at her college were convinced and agreed to provide funding for an EDR solution. Chen and her staff held a small celebration by videoconference. Then they got to work building the requirements for the solution, sorting through the options and implications that they will need to address to pull off this migration to an entirely new way of managing endpoint security.

What is it?

Endpoint detection and response (EDR) is the process of monitoring endpoint activity in real time, looking for digital threats and implementing measures to halt and remediate those threats. Endpoint devices include laptops, tablets, phones, and desktops, and EDR is one approach to shielding endpoints from cyberattacks. Conventional forms of endpoint protection, which include antivirus/antimalware tools and firewalls, protect against known threats. EDR, in contrast, also identifies novel threats and behavior-based attacks. Moreover, EDR can take active steps to mitigate threats, protecting the devices and systems connected to the network.

How does it work?

Conventional strategies for malware detection use a signature-based approach. Signatures are lines of code that uniquely identify software, and once a piece of software has been recognized as malicious, its signature can be added to a database of known threats. Signature-based tools such as antivirus/antimalware tools work alongside them—conduct real-time monitoring and analysis of events, looking for activities that might not be inherently suspicious but that vary from established or expected patterns of behavior. Once a possible threat has been identified, EDR tools can take steps to contain the threat, enable an investigation into it, and eliminate or remediate possible damage from it. Most EDR applications use machine learning and artificial intelligence, along with a cloud-based component, analyzing data from a wide variety of sources to further increase their ability to stay ahead of bad actors.

Who’s doing it?

As the types and frequency of cyberattacks have increased, colleges and universities have come to understand the inadequacy of conventional approaches to endpoint protection. Most institutions of higher education have at least begun to investigate new approaches, and many are pursuing EDR. Because EDR implementations can be complex, institutions are taking time to...
Endpoint Detection and Response

carefully develop their requirements for EDR and screen possible solutions. For example, some will deploy EDR extensively, on essentially every endpoint that interacts with institutional resources, whereas other institutions will limit EDR deployment to the most valuable and vulnerable endpoints. Meanwhile, many vendors of traditional antivirus products are moving into EDR, resulting in a healthy, competitive marketplace that offers numerous options, along with the overhead of choosing one.

4 Why is it significant?

An attack surface is all the points, both physical and digital, through which an attacker can try to gain access to digital resources. An organization's attack surface includes, among other items, all the endpoints connected to the network and its systems. Attack surfaces are expanding rapidly, in part due to the proliferation of user devices and in part as a result of the move to remote working/learning prompted by the pandemic. By some estimates, 70% of security breaches come through endpoints. A growing number of cyberattacks can evade conventional endpoint security tools, and those tools can do nothing once a breach has occurred. EDR provides significantly broader, more elaborate protection against the increasingly complex landscape of cybersecurity threats.

5 What are the downsides?

The far-reaching protection provided by EDR systems comes at a cost—these tools are exponentially more expensive than traditional solutions. Although EDR tools can save time and energy once implemented, they involve considerable overhead getting them up and running, including the time needed to install, test, and configure them to work well in an institutional setting. Cybersecurity applications interact with many other kinds of software on campus, and those interactions must also be taken into account when deploying EDR. Cybersecurity lives on a spectrum, involving tradeoffs between security and convenience, and endpoints will always be one of the most challenging areas of security vulnerability. Successfully deploying an EDR system requires accurately gauging campus culture and implementing security tools in a way that accommodates users' expectations for ease and simplicity of device and network access—no single deployment model is appropriate for all colleges and universities. In some cases, EDR requires different training and skills among IT staff, and some institutions will struggle with the amount of time needed to adequately support an EDR solution.

6 Where is it going?

Cybercriminals don't rest, and they will continue to look for new ways to compromise digital systems and assets. Colleges and universities need to protect data and systems that increasingly live in the cloud, adding new layers of complexity to cybersecurity. A growing number of organizations are turning to managed detection and response (MDR), an outsourced service that provides 24/7 monitoring and proactive threat detection. Extended detection and response (XDR) represents an evolution of EDR that extends protection across additional layers beyond endpoints, including email, networks, and cloud environments. Sometimes called "cross-layered detection and response," XDR provides greater visibility into security threats and deeper context for them, allowing security professionals to respond more quickly and thoroughly to cyberattacks. Just as antivirus tools are being replaced by EDR, so too will MDR and XDR and similar services further expand the range of cybersecurity defenses.

7 What are the implications for higher education?

Colleges and universities are an appealing and frequent target for cybercriminals, and as the stakes rise, so does the need for tools to protect an institution's digital assets. Campus-based information security can't protect the devices and users in remote teaching and learning environments, and phishing and other attacks are increasingly subtle and effective. At many institutions, the security unit is lean or under-resourced, leaving staff forever playing Whac-A-Mole against a torrent of threats. EDR systems can provide protection for the growing number of institutional endpoints from increasingly sophisticated and targeted cyberattacks. EDR can cover institutional assets, servers, and other sensitive resources, and it can also include student-owned devices. Institutions can decide how extensive they want the coverage to be and put together an implementation that balances cost, culture, usability, and protection.