THE END
OF YOUR NETWORK AS YOU KNOW IT

Protecting endpoints is more complicated than ever as the edge is everywhere
The ever-elusive endpoints

Even though there is a proliferation of endpoint protection tools, software, frameworks, and approaches to lock down network, in reality, protecting endpoints is just the tip of the iceberg. Allen Bernard reports.

Security professionals charged with protecting corporate endpoints face a dilemma. On the one hand, they have to make sure that the ever-expanding landscape of network endpoints are protected, but they also know that securing these devices is a bit of a lost cause. The reason is simple: Most security incidents are caused by human error. What they are really protecting is not the device but rather the organization's network and data.

It has become almost cliché that the castle-and-moat mentality of protecting the perimeter at all costs is no longer sufficient to keep attackers and hackers from infiltrating the corporate network and stealing the crown jewels. So, locking down endpoints and doing little else is not going to make anyone's network more secure. Frankly, that assumes you actually know where all the endpoints are and have physical access to them. Today that is not a given.

“You can put a lot of money into building up the castle walls and digging a bigger and deeper moat, and filling it with sharks,” says Robert Zahn, CIO and CISO of AAA of Ohio, “but if one of your employees opens the back door and lets the person in, all that money didn’t really help.”

This does not mean that you simply give unprotected and unauthorized devices network access; far from it. The reality is that the types of endpoints that make up a typical organization’s network edge are expanding rapidly. And these devices are getting “smarter.”

It was not too long ago that most CISOs were simply concerned with PCs, Macs, laptops, and a few smartphones. Today we see the proliferation of internet of things (IoT)-enabled smart devices such as consumer electronics, voice-controlled personal assistants, sensors, industrial control devices, and a myriad of other commercial and industrial devices. When you combine those devices with the increased dependency on third-party providers of software and services delivered via the cloud, the network edge has become so porous and fuzzy that, for some CISOs, it is not even something they talked much about anymore.

“I stopped using that edge terminology some time ago,” said Tremayne Smith, CISO at The Ohio State University’s Wexner Medical Center. “As soon as we started allowing remote access, that edge went away. For me there’s securing our network and securing our data.”

Not only does Smith have all of the typical laptops, PCs and smart devices to worry about, also under his charge are the hospital’s medical devices, which range from connected insulin pumps to MRI machines running on Windows PCs. With tens of thousands of employees, patients, doctors, and nurses, along with known endpoints that number in excess of 70,000, Smith cannot lock down all of these devices. As a teaching hospital, the medical center’s IT

OUR EXPERTS: Endpoint protection

Joey Cox, IT director, Central Ohio Primary Care
Justin Forbes, penetration testing team lead, CERT division, Software Engineering Institute, Carnegie Mellon University
Angelo Mazzacco, CIO, Central Ohio Primary Care
Stephen Mellor, CTO, Industrial Internet Consortium
Tremayne Smith, CISO, Ohio State University’s Wexner Medical Center
Robert Zahn, CIO and CISO, AAA of Ohio

$5M
Cost of securing endpoints after an attack in a large organization
– Ponemon
staff job is to equip the hospital’s staff with the flexibility and functionality they need to provide the best patient care they can.

“We’re a hospital and we’re here to take care of patients and do research,” he says. “We’re not a security company. So, if someone says they need a smart TV to talk to a database somewhere that puts the patient name up in the corner, that’s what has to happen.”

Given that the vast majority of cyberattacks are caused by someone downloading and running malware or having their credentials pilfered, these endpoints still require device-level security. At a minimum, they run device-level antivirus. Policies also keep devices from running tasks such as macros, while sandboxing and local detonation of suspicious executables also are employed.

“So app whitelisting and functionality whitelisting ... those are steps we have to take,” he says. “But we have to get into policy and exception management instead of just device

and network management. So, that means putting in end-user policies that protect them from themselves so they can’t make mistakes.”

Because some endpoints are more critical than others, the first step in any endpoint protection program is defining what an endpoint is. This sounds simple but given the ever-expanding and rapidly evolving ecosystem that is IoT, it can be overwhelming.

But, really, it comes down to just a couple of simple tenants, says Stephen Mellor, CTO of the Industrial Internet Consortium.

“Everybody has trouble trying to come up with a good definition,” he says. For Mellor, an IoT device and endpoint share a common definition: “A component that has computation capability and network connectivity.” That is it. So, regardless of whether it is a simple temperature sensor on a factory floor, a PC running an MRI machine, or a cloud provider’s server, by this standard, they are all network endpoints.

It is all about the network

While there are too many tools, software, frameworks, guidance, and advice for securing endpoints to list here, the common thread that seems to run between them as making sure that the device, application, or user are who they say they are before granting them access to the network and its applications. And then, the experts agree, only grant them access to the applications and data that they absolutely must have. In this way, the network and the data are protected even if the endpoint is compromised.

Of course, this is easier said than done since a great many, perhaps most, organizations today have no idea of how many or what type of devices are connected to their network. Many also lack the internal controls in place to prevent an attacker, once inside the network, from moving laterally from one system to another.

This is something most hackers find easy to do, says Justin Forbes, penetration testing team lead in the CERT division of the

8500%

Coin miners on endpoint computers increased by 8500% in 2017

– Lloyds Bank
Software Engineering Institute at Carnegie Mellon University.

“When I conduct pen tests we see it all the time,” he says. “Anytime an organization has a standard image and they use the same local admin password on all those images, as soon as we compromise one system, it’s usually minutes to hours max before we compromise the whole network.”

So, instead of relying on perimeter defenses, a lot of organizations are moving towards a zero trust approach to endpoint security. Basically, zero trust means you assume that the endpoint and the user are untrustworthy from the start. This frees up resources to focus on securing more important assets like servers and data instead of having to secure on every single user laptop, smart phone, or workstation.

“You don’t care if someone is coming from a phone or a library laptop so long as they are using multifactor authentication,” says Forbes.

Once users are on the network, user access controls and fine-grained network segmentation limit where they can go and what data and applications they can access. Zero trust would have gone a long way, says Forbes, to contain the NotPetya virus given that it moved from system to system based on weak administrative controls.

The beauty of system like zero trust is that it works regardless of device or network type. So in industrial, machine-to-machine (M2M) IoT environments where sensors and actuators often communicate using plain text protocols and control system operating systems are unpatched and out of date, it would work just as well.

Zero trust is a big part of Smith’s endpoint strategy. Why would a SharePoint admin need to have access to confidential data? Why would a nurse who is checking her schedule from a coffee shop need to access a patient’s medical records from her phone or laptop?

“I want those transportable polices to go with users to really segment and compartmentalize those users who, when they need to access something they can, and when they don’t, they can’t,” he says. “It’s going to help my haystack not be as big of haystack when I’m looking for something malicious that occurred.”

Smith also uses Active Directory to set group polices for PCs so they can only authenticate and talk to other whitelisted devices on the network. He relies on mobile device management (MDM) software to set and enforce similar policies on mobile devices. He also requires two-factor authentication for network access and limits most BYOD (bring your own device) to guest networks.

Of course, there is no panacea — no one perfect approach that secures everything all the time. Even the increasingly popular unified endpoint management (UEM) platforms, which connect to and manage all of a company’s endpoints, can become a single point of failure if incorrectly configured. If a hacker gets access to these systems, they have access to all the endpoints, says Forbes. Aware of this issue, some UEM vendors advise customers to

---

“75% Percentage of data breaches caused by external attackers


You would be amazed at how many people have ‘admin’ as their password”

– Stephen Mellor, CTO, Industrial Internet Consortium
isolate their UEMs from network domains. “Everything has its pluses and minuses,” says Forbes. “Having something like UEM makes it a high-value target for a hacker.”

But, if zero trust policies and practices are in place, even this type of attack would not get very far, hence its growing popularity.

**Deploying defense in depth**

“If you want to secure your endpoint you have to shore up your access tools and identity management,” says Joey Cox, IT director of Central Ohio Primary Care (COPC), the largest physician-owned primary care group in the country with 80 offices. “We really approach security from a layered standpoint because you can’t count on a tool to work every time. If you don’t have layered security, you don’t have endpoint protection because you haven’t addressed the people problem or the access problem.”

Cox’s defense-in-depth approach leans heavily on identity and access management (IAM) principles and tools. After risk profiling all of the devices on their network, his first layer of defense starts with network access control (NAC) and network access protocol (NAP) to ensure a device’s defenses and OS are up-to-date. He also encrypts all of the network endpoints.

To keep hackers from accessing admin accounts, the medical group uses a tool that looks for suspicious activity and reports it back to the security information and event management (SIEM) system, which serves as the focal point and single-pane-of-glass control panel for all of the different tools and security software running on the network.

Cox also uses AI-based anomaly detection tools to spot suspicious network traffic. His servers are outfitted with clients that monitor who has access to the server and its applications. That way he can uncover end users that do not need to have access to specific servers and applications and then block them.

He also employs network segmentation to isolate his servers, printers and fax machines (healthcare still relies on faxes) from the rest of the network. He says he has tools in place to mitigate 100 percent of all ransomware, one of the biggest cybersecurity problems facing healthcare providers today.

As an added layer of security, Cox, like Zahn at AAA, does not allow non-approved or user-owned devices from accessing the network, so no BYOD issues. COPC even blocks BYOD-friendly partners from accessing confidential patient data.

To keep track of protected health information (PHI), Cox employs a data loss prevention (DLP) tool that attaches a fingerprint to PHI data so that it can be tracked and a chain of custody established. If data is found on an unsecured device, the tool lets him delete the information while leaving a text file behind telling the user where they can find it.

To counter cloud security concerns, Cox is deploying a cloud access security broker (CASB) server. CASBs serve as an authentication gateway that sit between a company and its cloud provider. CASBs allow network administrators to enforce policies such as two-factor authentication and whitelisting, as well as set device-level

---

**77%**

Percentage of companies that said they did not have a formal cybersecurity incident response plan

– Ponemon The Third Annual Study on the Cyber Resilient Organization, March 2018

---

If you want to secure your endpoint you have to shore up your access tools and identity management

– Joey Cox, IT director, Central Ohio Primary Care

---

Robert Zahn, CIO and CISO, AAA of Ohio
policies before access to applications and data on the cloud is allowed. Not only does this give Cox the ability to block entire regions based on IP address (so if China or Russia is trying to use brute force password attacks from regional IP addresses for those regions, he can simply block them), it keeps the cloud provider’s administrators from compromising his security by either having their passwords compromised or selling them to the highest bidder.

“What you’ve done is you’ve moved the network edge to the cloud,” says Cox. “If they can breach your user name and password in the cloud then they now have a user account that will work internally on your network. And that’s the one piece no one really thinks about.”

They even use encrypted texting so their doctors do not have to stop what they are doing and find a workstation somewhere to communicate with colleagues. Finally, they employ penetration testing vendors and change vendors every six months so that they get a fresh set of eyes on their network. They also spend a lot of time training users not to click on links in their email.

What keeps them up at night

Even with all this security in place, COPC’s CIO Angelo Mazzacco still worries. “What really keeps me up is we have a very important obligation to our patients to keep information about them secure. That could be the difference between someone losing their job if the information got into the wrong hands. Each night you’re going to have some thoughts about that as you go to bed: Have you done everything you can do to keep their information secure?”

For AAA’s Zahn, his biggest concern revolves around the new employee that just does not know any better. There are always “super clickers” out there, he says, that no matter how much you train them, they invariably click on a malicious link. “That is what starts all of these attacks,” he says. “Since I can’t control all 650 individual employees, I have to protect the data at rest.”

Zahn also employs MDM and uses outside vendors to monitor his network. He recently adopted the National Institutes of Standards and Technology (NIST) Cybersecurity Framework guidelines to ensure they are doing everything they can to keep customer information safe and is in the process of getting them implemented – a non-trivial task given there are 475 boxes on the checklist.

What keeps IIC’s Mellor up at night is ignorance. That is the biggest threat, he notes. With attacks coming from all over — from nation states to script kiddies — and new attack vectors and techniques surfacing almost daily, it can seem impossible to keep up. But most attackers still rely on the basics to get in: unpatched devices and phishing. Why? Because it is easy and it works.

“You would be amazed at how many people have ‘admin’ as their password,” he says. “If I were the CISO of any large business, I wouldn’t sleep at all,” says Mellor. “There are a lot of threats out there.”

For more information about eBooks from SC Media, please contact Stephen Lawton, special projects editorial director, at stephen.lawton@haymarketmedia.com.

If your company is interested in sponsoring an eBook, please contact David Steifman, VP, publisher, at 646-638-6008, or via email at david.steifman@haymarketmedia.com.
Carbon Black.

Carbon Black (NASDAQ: CBLK) is a leading provider of next-generation endpoint security delivered via the cloud. Leveraging its big data and analytics cloud platform – the Cb Predictive Security Cloud – Carbon Black consolidates prevention, detection, response, threat hunting and managed services into a single platform with a single agent and single console, making it easier for organizations to consolidate security stacks and achieve better protection. As a cybersecurity innovator, Carbon Black has pioneered multiple endpoint security categories, including application control, endpoint detection and response (EDR), and next-generation antivirus (NGAV) enabling customers to defend against the most advanced threats. More than 4,600 global customers, including one-third of the Fortune 100, trust Carbon Black to keep their organizations safe.

For more information, visit https://www.carbonblack.com/