How to Meet Your Customers' Endpoint Security Needs

Table of Contents

Explaining what we mean by endpoint protection

Endpoint security refers to securing endpoints or end-user devices like desktops, laptops and mobile devices. Endpoints serve as points of access to an enterprise network and create entry points that can be exploited by malicious actors.

When we talk about endpoint protection, we are talking about protecting these endpoint devices from cyber threats. By and large, cybersecurity services for most organizations are about protecting access to data and systems. Data and digitalization have become a double edge sword. On the one hand, it allows organizations to disrupt and reimagine even established markets. On the other hand, the data itself contains such incredible value, it makes the guardians of the data an attractive target for cybercriminals.

So, when it comes to endpoint protection, the underlying goal is to keep your customer's organizational data and systems safe from threats. They will also look to prevent endpoints belonging to employees, suppliers or third parties from compromising corporate data and systems. It is important to stress that endpoints don't always have a visible user interface. For instance, a temperature sensor connected to the corporate network is a form of an endpoint. A router on an employee's home network could also be an endpoint. As such, devices with access to organizational systems and data need to be considered part of an organization's cybersecurity posture.

What are the endpoint threats facing businesses?

IT networks expand as employees and the business connect more and more devices. Every endpoint represents an additional attack surface for a cybercriminal. These cybercriminals themselves come in all shapes and sizes and are motivated by different reasons. For the most part, cybercriminals are either trying to access/steal organizational data or trying to disrupt the organization.

When it comes to cybercriminals, the mainstream media frequently portrays a stereotype that's misleading and unhelpful. Many cybercriminals are highly organized and well-resourced criminal organizations with a clear purpose and objective. Some groups are even sponsored by nation-states. A determined and professional cybercriminal will often have spent days, weeks, or even months studying their target's cyber posture before an attack. They will analyze the endpoint to find a known or new vulnerability to exploit their desired outcome. Furthermore, they will go to extreme lengths to remain undetected inside a corporate network until they are ready for you to know of their existence.

It should be noted that not all threats are external. Sometimes threats can come from disgruntled employees. Other times your endpoint protection is about preventing simple mistakes and bad cybersecurity hygiene. For instance, working on a sensitive spreadsheet on a public Wi-Fi in a coffee shop without encryption. There is no malicious intent, yet you still want to protect the sensitivity of the organizational data.

When optimizing an organization's cybersecurity posture around endpoints, it is unrealistic to expect to create a cybersecurity posture that's 100 percent secure. Instead, you are looking to make sure the organization is not an easy target and provides the cybercriminal with very little return for their effort.

Hackers use a variety of methods to attack an endpoint. Some common examples include:

- **Ransomware** - A type of malicious software designed to block access to a computer system until a sum of money is paid.
- **Vulnerability exploits** - A code that takes advantage of a software vulnerability or security flaw. When used, exploits allow an intruder to remotely access a network and gain elevated privileges or move deeper into the network.
- **Phishing** – Criminals dangle a fake lure (an email that looks legitimate) hoping users will 'bite' by providing the information the criminals have requested.
- **Drive-by downloads** – An unintentional download of malicious code to a computer or mobile device that leaves it open to a cyberattack.
- **Watering holes** - Security exploits where an attacker seeks to compromise a specific group of end-users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment.

- **Weaponization of adware networks** – Adware has become more than just a minor nuisance. Traditionally, adware only showed advertisements. However, newer forms of adware have techniques to improve their ability to persist on a host and infect more machines.

- **Denial of service attacks (DOS) -** Endpoint DoS is an attack type focused on blocking service availability to users without saturating the network that provides access to said service. This attack is performed by either exhausting host system resources to block the service or by instigating a crash on the host system.

- **Bots** - A bot, short for "robot," is a type of software application or script that performs automated tasks on command. Bad bots perform malicious tasks that allow an attacker to remotely take control over an affected endpoint. Once infected, these devices may also be referred to as zombies. "Thingbots" is a new kind of botnet that incorporates independent connected objects with the purpose of remotely taking control and distributing malware.

- **Man-in-the-middle attack** - This is a particularly dangerous attack where a hacker interrupts and breaches the communications between two separate systems. They secretly intercept and transmit messages between two parties when they believe that they are communicating directly with each other.

- **Exploiting poor password management** - According to First Contact, 23 million account holders still use the password, "123456." Other users still rely on common passwords including "qwerty," "welcome" and "admin." Why? Because they were default passwords that hadn't been changed once the device was set up on the system. Cybercriminals know these are the defaults, so you are extremely vulnerable if you don't amend them. Poor password hygiene represents a major risk.

Attacks come from different vectors:

- The Web is the way attackers usually come at an organization. It provides an easy way to spread links to hosted malware via email and the use of IM. The hackers use command and control servers to manipulate botnets, plus they install components after infection for multi-staged attacks. Attacks can be highly sophisticated; some malware attacks use polymorphic and metamorphic techniques.

- Employees are a popular attack vector that cybercriminals will leverage. Insider attacks, whether accidental or indeed malicious, make up 70% of cyberattacks, and usually originate from within the firewall perimeter. Because many firewalls are outward facing, an attacker with an already established connection can exploit vulnerabilities in traffic. The attacker will use advanced sociology and behavior profiling to lure in intended victims. Experts will often state users' behaviors determine the success or failure of an endpoint security strategy. Therefore, employees need to participate in regular endpoint security training.

- Applications connecting to the network that aren't sanctioned by the IT department are known as Shadow IT. These pose a risk because they're either not known about or pose additional difficulty when it comes to management. Shadow IT examples include IoT initiatives managed by facilities managers and wearable technology brought in by employees or guests.

- If the firmware on a device is fixed and immovable, it's a sitting target! Attackers can dissect it at their leisure, develop more threats and launch attacks they know will work on every example of the device. The VPNFilter attack, launched in May 2018, is an example of what can happen when an entire category of device cannot update, or, even more worryingly, users are unable or unwilling to apply the available updates. Security best practice demands that, if a device can be updated, it should be kept up to date on patches and revisions. When it comes to devices that can't be updated, there's still no excuse, as keeping up with known vulnerabilities is crucial. Once you've done this, it's just as important to ensure another security layer blocks these vulnerabilities.

- BYOD mobile devices are another very common attack vector. Non-premise devices reduce visibility in a network. Plus, devices could go unprotected or unmonitored for months at a time, with data passing through these devices without any form of regulation.

- The Internet of Things (IoT) is also a common attack vector because they rarely, if ever, have cybersecurity protections on their firmware or software. Due to their nature, they are frequently the blind spots on an organization's network, allowing hackers to use them as stepping stones to more profitable targets. We are also seeing more operational technology (OT) becoming connected to the internet as part of industry 4.0. Machinery used in factories and industry was traditionally stand alone and isolated. This industry doesn't have decades of experience in battling cyber threats like the IT industry. Cybersecurity is not part of their DNA. Yet, if a cybercriminal's objective is to disrupt an organization, attacking the OT is like hitting the jackpot.

- Compromised Wi-Fi and domestic devices are also an attack vector. Poorly secured gateways make information theft easy. Adversaries can hijack the Wi-Fi connection, inject malicious code, take control over systems or access data. One of the challenges we've seen with many home workers is the fact the domestic routers and networks offer nowhere near the sort of security and protection as those used in enterprises. Sometimes the vulnerability doesn't come from the router itself, but the other devices that were running on the home network. In a typical home, you might expect to see a smart TV, a wireless printer, video game consoles, wearable devices, personal phones, smart lighting, smart doorbells, or all manner of devices sharing the network. Other devices from friends and family may occasionally connect to the home network when they pay a visit. These all represent vulnerability and offer the cybercriminal a stepping stone to their ultimate target. There is a strong argument to help employees, particularly high target employees, make their home networks more secure and encourage better cybersecurity hygiene with personal devices. In this way, we see a blend between personal and work, where a weakness in one area makes the other vulnerable.

- An often-overlooked vector is a port on the endpoint device itself. Hackers have been known to plant infected USB keys and drives to transfer the virus directly to the device itself. The next attack vector to mention here is applications. Cybercriminals either embed malicious code into mobile applications, or they look to exploit weakness and vulnerabilities in applications that have not been written according to best practice.

- Threats can take various forms from information warfare campaigns to espionage to control of critical national infrastructure. The tooling is at a whole other level of sophistication and is more accurately described as cyber weaponry. Nation-state attacks increased from 12% to 23% in the past year, according to Verizon's 2019 Data Breach Investigations Report. In recent years, large-scale cyberattacks have been attributed to state-sponsored groups. Interestingly, there is evidence to suggest that the testing ground for cyber weapons are the less developed countries. Here the attacks are honed and perfected before being deployed against developed countries and the true intended targets.

Once the cybercriminal has compromised the endpoint, they will use the endpoint to either:

1. **Enter the organizational network.** One of the mistakes organizations make is thinking that an employee working from home on their laptop is safe using a VPN. A VPN is simply a tunnel. Even if it is encrypted, if the attacker has compromised the laptop, they can access the organizational networks through the laptop and its VPN. Hence the focus on preventing endpoints from being compromised in the first place.

2. **Hijacking the device to launch a distributed denial of service (DDos) attack on the organization itself**. If a hacker can take control of a trusted device, their ability to launch devastating denial of service attacks is magnified, unless the organization puts in place the right endpoint protection.

What's making your customers do something about endpoint protection?

Most people will agree it's obvious it's in the company's interest to protect its data and systems. If it loses its data, it can lose its IP. If it can't access its systems, it stops trading. Organizations spend time, resources and capital building up data to the point that many people argue the data should appear on the balance sheet as an asset. However, the question becomes to what degree they should protect the data?

Companies who possess high-value data are not always free to decide to what degree they protect the data. Possession is not always the same as ownership, especially when it comes to personal data. Who owns personal data? Is it the physical person to whom personal data relates, i.e. the data subject? Or is it the company that invested time and money on collecting, creating, refining, analyzing and understanding the personal data to create great products and services for its customers?

The GDPR does not explicitly give us an answer to personal data ownership. However, many legal experts argue that personal data is owned by the data subjects rather than the data controller. Consequently, organizations have a legal and moral obligation to protect data in their care by adopting a strong cybersecurity posture. In addition to GDPR, most countries have their own data protection legislation.

Data and the need to protect it is one of the key drivers of cybersecurity. Find an organization with lots of high-value data, especially if it is sensitive, and you'll find they have a compelling need for cybersecurity. A strong cybersecurity posture depends on having robust and well-thought-out cybersecurity strategies. The starting point is having a clear understanding of the data your protecting. In particular:

- How much data is there?
- Who owns the data?
- Who is the data subject?
- How is it being collected?
- How is it being transmitted?
- How is the data being accessed, from where and by who?
- How is it being processed?
- Who is the data being shared with and why?
- How is the data being maintained?
- How is it being stored?
- What are the legal and regulatory requirements around the data?
- How is the data disposed of at the end of its lifecycle?

When you have a clear picture of the data you're protecting, you can start to understand the cybercriminals' possible motives and strategies. When you know this, you know where to focus your efforts on protecting endpoints against cyber threats.

Why companies outsource endpoint security

There are several compelling reasons why companies are looking to service providers to help them with endpoint security. Here are some of the main considerations . . .

Companies often don't fully understand the true nature and extent of the threats they are facing

One of the first challenges companies have is understanding just how vulnerable they are. Cyber is being called the world's first frictionless weapons system. The moment a new type of attack is released and discovered, everybody's knowledge is tested. Then the cybercriminals morph the attack and come back in different ways. Sometimes there is an assumption that the application providers have built-in more security than they have. Or if security is built-in, there is a misunderstanding that security is limited/optimized to the vendor's own application. Sometimes there's a denial tendency because up until this point, they have gotten away with a relatively weak cybersecurity posture without consequence. It is important we're careful not to be over-critical here, many end users don't know what they don't know. It's the role of the security experts to show and guide them.

There is a real incentive to lower the threats from endpoints through proper management and endpoint protection

The latest Verizon 2020 Data Breach Investigations Report reported that 82% of attacks compromised systems within minutes. However, the more concerning figure from IBM's Cost of a Data Breach Report is that in 2019 it took on average 206 days for the organization to identify a breach. It then took a further 73 days on average to contain the breach. The longer the cybercriminals are in, the higher the risk. Given this information, it is not surprising organizations are desperate to ensure endpoints aren't open doors for the criminals to walk through. A lack of proper investment in endpoint protection undermines cybersecurity investments for the rest of the IT estate.

Cyber threats are continually evolving

There isn't just one type of threat. So, even if you implement one type of solution, it is not a case of walking away and thinking the job is done. Cybersecurity measures need to be managed and updated to protect against new forms of threats. This is hard for companies whose main business focus isn't cybersecurity or even technology. Again, this is another area where you can step in and provide expertise to help these companies maintain a strong cyber posture.

Cyberattacks have become more sophisticated and specialized

Over the years, cybercriminals have developed a very diverse range of tactics to exploit vulnerabilities. The expertise around combating these threats has become a series of sub-disciplines within cybersecurity, in much the same way as science has its own sub-disciplines. Here's some examples:

- Access control
- Anti-keyloggers
- Anti-malware
- Anti-spyware
- Anti-subversion software
- Anti-tamper software
- Anti-theft
- Antivirus software
- Cryptographic software
- Computer-aided dispatch (CAD)

Endpoint protection

- Firewall
- Intrusion detection system (IDS)
- Intrusion prevention system (IPS)
- Log management software
- Parental control
- Records management
- Sandbox
- Security information management
- SIEM
- Software and operating system updating.

Good cybersecurity relies on having the right knowledge and tools to keep cybercriminals out. The consequence of this is that the market has become very fragmented with cybersecurity vendors constantly innovating to offer the best protection in their sub-discipline.

Detection is hard

In the early days of computer viruses, you were aware the computer had a virus. Today, the opposite is true. Cybercriminals deliberately design their attacks so that the deployment of the payload won't be detected. Consequently, to detect an attack in its early stages, you need to understand the signs and know what to look for. If an endpoint is behaving in a certain way or shows signs of malicious intent, you need the right endpoint protection in place to stop the threat in its tracks. This is where having quality cybersecurity tools and experts who know how to use them plays a critical role.

IT estates have become far more complex and nuanced with many more attack surfaces

Digitalization has transformed the shape and size of IT estates beyond recognition:

- **The rise in users and stakeholders** - Where once a user might have been an employee, today, an application user might also consist of suppliers, customers and even AI applications. This means more endpoints of different types trying to access organizational data and systems. The challenge for organizations is to let the right people access the right data at the right time on the right devices, all while keeping the criminals out.

- **Locations** – Employees expect to be able to work from anywhere with a signal at any time day or night. This creates its own set of security considerations for endpoint management.

- **Devices -** Long gone are the days where the IT department only had to be concerned with desktops and servers. Just about everything these days seems to be internet enabled. Businesses are seeing a huge rise in internet of things (IoT) devices. Building control systems, not to mention operational technology on the factory floor, are becoming internet-enabled. Every one of these devices generates, processes or transmits data. For cybercriminals, these represent vulnerabilities and possible entryways. Devices run on a host of platforms such as macOS®, Linux®, iOS, and Android™. For the business, these represent a huge headache in making sure they are all patched and updated. It also makes it far more complex for companies to manage and control. Also, endpoint devices out in the field are vulnerable to physical theft. Consequently, there is a whole exercise that needs to be conducted around user password management and encryption. As an extension of this, companies need robust processes for changing the default admin passwords on endpoint devices.

- **Company data and infrastructure is hiding everywhere.** One of the challenges with modern data driven companies, is keeping tabs on all the places where the data resides. Most companies are very conscious about sensitive data residing on endpoint devices, especially if they are unmanaged. However, there is an additional consideration here. Gartner studies have found that Shadow IT is between 30 to 40 percent of IT spending. According to Netskope, the average large enterprise uses over 1,249 cloud services, and less than 2% are managed by IT administration. When company data finds its way onto Shadow IT infrastructure and applications, it doesn't have the same controls. It is easy for the data to find itself on endpoint devices. If the company is unaware of the shadow IT, it may be unaware that it needs to also protect the data being exchanged with the application. As trusted advisors, solution providers play an important role in helping companies identify areas where corporate data might be hiding.

Global skills shortage of security experts

70% of ISSA members believe their organization has been impacted by the global cybersecurity skills shortage. Cybersecurity is not one of those areas where you can try and fudge your way through; you really do need expert knowledge - Absolute Software's Endpoint Security Trends Report found that the more complex and layered the endpoint protection, the greater the risk of a breach. Overloading every endpoint with multiple agents is counterproductive and leaves endpoints less secure than installing fewer agents. The value of the data, along with legal and industry regulations, means that doing nothing is not an option. Some larger companies will employ their cybersecurity experts. Others will outsource this function to their preferred IT or cybersecurity provider.

The fragmented nature of the cybersecurity market

The cybersecurity market is known for being highly fragmented. There are thousands of different technology vendors and products, each designed to help a business improve a particular aspect of its cybersecurity posture. Understanding what products to use, where to use them and how to implement them effectively requires detailed knowledge of the cybersecurity market. This is where providing endpoint management can remove so much of this headache. It can free up the business from spending months and months researching the best products, solutions and services to combat the endpoint threats.

Combatting cyber threats requires a cultural change in most companies

Technology is only part of the solution. Cybercriminals are deliberately deceptive and deceitful. A company's employees benefit from a constant training, so they can better identify cyber threats. Cybersecurity providers can help identify vulnerable users and implement an education program.

Fortunately, Tech Data's Cyber Range team of solutions-focused experts is here to help position you provide such training through:

• Expert Resources: Tech Data provides expert resources with significant industry tenure. In fact, our team of solutions-focused (vendor agnostic) business development resources is larger than any other distributor.

• Access to Essential Cybersecurity Skills: We provide highly skilled and diverse security technical resources to support your security team.

Companies are more effective when they focus on what they are best at

Not all companies exist to be cybersecurity experts. Every company has limited resources. If a retail company built up the in-house expertise to become a world leader in cybersecurity, the chances are, they're not focusing on their core business. Outsourcing cybersecurity to a trusted advisor makes a great deal of sense, especially if it frees up bandwidth and resources to work on more innovative projects that leverage next-generation technologies to drive its core business to the next level.

Freeing up bandwidth for the internal cybersecurity team

Successful businesses are continuously pushing ahead with new initiatives and digitalization projects. In this context, having the dedicated in-house cybersecurity experts tied up on routine tasks, such as endpoint protection, might not be the best use of their precious bandwidth. Savvy organizations will be considered and measured when it comes to utilizing their experts. Hence, outsourcing certain routine tasks to a trusted Solutions Provider, means the in-house experts have more bandwidth to focus on innovative business initiatives that will impact the bottom line.

A company's cybersecurity posture is forever changing

One of the challenges for companies that try to serve their needs in house is that their cybersecurity posture is not fixed. For instance, when the COVID-19 pandemic hit, many companies were forced to ensure employees could work from home. Equally, when lockdown measures started to relax, businesses found they had a mixture of employees still working from home and working from the office. This change in an organization's footprint has an impact on its cybersecurity posture. In response, endpoint security policies need regular reviewing and tweaking.

Even when times are less dramatic, companies still invest in new technology, acquire new organizations and undertake short-term projects. These situations require a level of cybersecurity agility that can be difficult to accommodate with an in-house team. A solutions provider is likely to be more flexible in terms of scale and evolve with new threats. Therefore, it becomes a case of simply upgrading the customer to additional new services from the portfolio as and when they are needed.

Patching and updating isn't as easy as it sounds

When a company rolls out an update, they need to check compatibility. Otherwise, it could impact usability, performance, and in a worst-case scenario – result in unplanned downtime. The average time to apply, test and fully deploy patches to endpoints is 97 days. This leaves a long window of vulnerability. Companies are wise to layer in additional endpoint protection if they know there are windows of vulnerability like this.

How do you convince your customers to invest in endpoint protection solutions?

A cybersecurity posture is all about a company's attitude to risk

In the past, whenever a cybersecurity threat was identified, a company would respond by purchasing the latest cybersecurity fix and plugging it into their IT estate. This approach was fine when the IT estates were relatively simple and small. However, technology has become pervasive throughout the organization, meaning modern IT estates are far larger and more complex. In parallel, the threat landscape has evolved at such a rapid pace, it is virtually impossible for an organization to have full visibility of all the cyber threats it faces. With more of an organization's processes automated, security incidents can be much bigger and more serious.

Plus, cybercriminals have industrialized trading skills, tools and knowledge on the dark web. Modern threat tools, some of which are AI-based, make detection incredibly difficult. Attacks slip through defenses and organizations might run the risk of not even noticing.

Making a company invulnerable to an attack has become a question of how much an organization is prepared to invest in better people, processes and tools to give them an integrated view of the IT threats and protection for the IT estate. However, there comes a point where investment becomes uneconomical. Therefore, organizations need to take a position on how much they are prepared to spend versus what they are trying to protect. Thus, they settle on a cybersecurity posture based on their attitude to risk. This position is very different for each organization.

Fail to take the right approach to cyber threats, prepare to risk going out of business

Security is a mindset that needs to go from top to bottom. It needs to become a level of habit rather than a simple tick list. Complacency over cybersecurity is dangerous. Data breaches exposed more than 15 billion records in 2019. More than $3.5 Billion was lost to cyber crime globally in 2019. The evidence couldn't be clearer; companies that fail to achieve a strong cybersecurity posture risk going out of business. Fines, brand damage, loss of IP and loss of customer confidence are just a few of the reasons why some companies who suffer a cybersecurity breach never fully recover.

Keep in mind the following additional factors when building a business case for endpoint security:

- **The penalties for non-compliance to industry-specific laws can be excessive, with repeat offenses leading to $1M or more in fines and long-term loss of customer trust and revenue.** Building a business case for endpoint security needs to factor in the potential non-compliance fees and penalties companies face for not having autonomous endpoint security. The Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), California Consumer Privacy Act (CCPA) and other laws require audit reporting based on accurate endpoint security data.

- **Endpoint Security ROI estimates fluctuate.** Pilots are a great way to build an evidence-based business case.
- **Be clear about articulating the benefits and gain C-level support.** It's often the CISOs who are the most driven to achieve greater endpoint security. Today with every business having their entire workforce with the ability to work virtually, there's added urgency to get endpoint security accomplished.
- **Use clear real-time dashboards.** Everyone should know what success looks like. Having a digitally enabled dashboard that clearly shows goals or objectives with progress is critical.

Show customers you can become their trusted advisor

Based on standards and security frameworks, such as ISO 2701 and NIST, skilled IT providers can guide their customers to navigate their way around cybersecurity threats. By helping organizations secure their IT infrastructure and their organizational data, you'll become core to their digital transformation journey and therefore their trusted advisor.

How do you get started with providing your customers endpoint security? Contact Tech Data.

Tech Data Security Solutions address the critical needs of the partners – offering complete, scalable solutions supported by tenured security professionals, delivered in a collaborative manner, creating immediate value for partners and end-users.

- Build Your Business: Protect end-users organizations with thorough security solutions.
- Extend Teams: Cybersecurity professionals are difficult to find and harder to keep. Tech Data's professional security team is available to make you successful.
- Rapid Results: We provide access to experts to grow your business quickly.

Expand your business and build deeper customer relationships with Tech Data's Security Solutions – comprehensive business solutions comprised of world class vendors and cybersecurity professionals.

Cybersecurity solutions and services will continue to be in high demand. We're here to be your trusted advisor and help customers avoid business disruption by providing the best and latest security technology and expertise.

For more information on how Tech Data can help you provide endpoint protection for your customers, please contact us at securityservices@techdata.com or visit techdata.com/security.