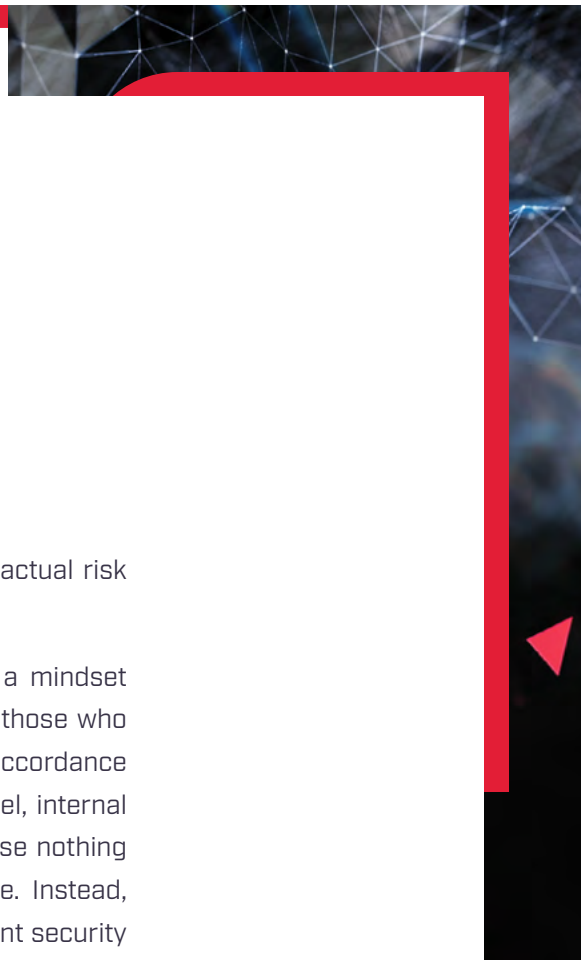
BUYER'S GUIDE TO ENDPOINT PROTECTION PLATFORMS IN 2020:

FEATURES YOU NEED FOR REAL-WORLD SECURITY IN TODAY'S THREAT LANDSCAPE

COMODO



IT'S NO SECRET THAT ENDPOINT PROTECTION IS THE MOST CRITICAL COMPONENT IN YOUR IT SECURITY TECHNOLOGY STACK.

After all, the majority of enterprise data breaches begin with the compromise of an endpoint device—more than 70% of them, according to data from IDC Research.[1] And as business IT environments grow increasingly complex, incorporating growing numbers of endpoints and new device types, the risk that one of these devices will become an attacker's entry point is skyrocketing.

Choosing the right solution to protect your organization's endpoints is no easy task, however. Though the vast majority of companies have already implemented some type of endpoint protection, the rate at which data breaches are occurring, along with how much these events are costing their victims, continues to climb.

The Ponemon Institute reports the average total cost of a data breach in the United States now tops $3.9 million.[2] But despite the fact that overall IT spending is at an all time high and there are hundreds of endpoint security tools available, actual risk exposure has increased.[3]

What's needed to reverse this troubling trend is a mindset shift. The most successful IT security leaders are those who have adopted—and designed their architectures in accordance with a Zero Trust Paradigm. In the Zero Trust model, internal 'trusted' zones with networks are abolished because nothing should be trusted unless it has been proven safe. Instead, ongoing verification and monitoring and omnipresent security controls are implemented.

Keeping Zero Trust's central premise in mind—that no data or network traffic is to be deemed "secure" without verification—and considering the key trends and emerging challenges that organizations must contend with as they build their security infrastructures, we can identify the most important elements an endpoint protection platform needs to include if it is to deliver positive return on investment (ROI) and boost resilience against today's attacks.

FIVE KEY CYBERSECURITY CHALLENGES OF 2020:

CHOOSE THE RIGHT ADVANCED ENDPOINT PROTECTION PLATFORM

The primary reason businesses aren't realizing the value they'd hoped for when investing into endpoint protection platforms is that attackers are constantly evolving their techniques and strategies, and the vendors of traditional endpoint security solutions haven't been able to keep pace.

It's critically important that you choose an advanced endpoint protection platform designed for today's cloud-based, distributed and diverse IT architectures—not the legacy environments of yesterday. And, it's vital that your endpoint protection offer powerful defenses to counter the attack strategies that are currently in widespread use—as well as proactive safeguards against whatever the future may bring.

Let's take a look at the top cybersecurity trends of 2020, and how they translate into must-have features for your endpoint protection platform.

FOR TRULY COMPREHENSIVE AND ROBUST DEFENSE IN THE CURRENT THREAT LANDSCAPE, AN ADVANCED ENDPOINT SOLUTION MUST:

1. Be purpose-designed for use in **Zero Trust** environments and offer a means of containing 100% of unknown files and runtime executables.
2. Integrate **multiple methods of detecting malware** as well as malicious scripts and fileless attacks.
3. Seamlessly extend **visibility and control** across multiple device types and platforms.
4. Simplify deployment and monitoring with a **cloud-native architecture**.
5. Combine the capabilities of **expert human analysts** and advanced algorithm-based analytics to maximize its ability to detect malicious activities quickly.

1

WHAT YOU NEED IN AN ENDPOINT PROTECTION PLATFORM:

BUILT-IN ZERO TRUST CAPABILITIES

An authentic Zero Trust-based approach is one that prevents unknown files from executing *at all times*. This includes PowerShell scripts and other fileless attacks, as well as traditional malicious software files. If a solution allows unknown files to execute in order to test their behavior and then determines whether or not those files are potentially malicious, your environment is put at risk each time its decision-making process operates.

Look for a solution that contains all unknown files immediately in a virtualized sandbox environment, allowing them access to host system resources and file stores only after they've been deemed safe through a comprehensive verdicting process. Ideally, verdicting should be quick, and performance (and with it, end user experience) unaffected by the containment process.

ATTACKERS ARE TAKING GREATER ADVANTAGE OF ARTIFICIAL INTELLIGENCE (AI), MACHINE LEARNING (ML), AND PREDICTIVE MATHEMATICS. DEFENSES MUST EVOLVE ALONG WITH THEM.

Though automation can bring numerous benefits to business, it's also giving rise to new kinds of attacks. Automation makes it effortless to launch attacks, like credential stuffing, that are challenging to accomplish manually on a large scale. It enables sophisticated malware strains to "learn" about systems' typical behavior so they can dwell undetected in enterprise networks for months or years. And, it makes it possible to put tireless machines to work sifting through enormous amounts of data in search of software vulnerabilities.

Security experts are currently seeing dramatic increases in the volume of automation-based attacks, and the math favors their success.[4] In order to be successful, defenders must stop 100% of attacks to prevent their networks from being breached. If attackers succeed only one time in every 10,000 attempts, they'll still end up compromising your environment.

The rise of automated attacks has made it more pressing than ever to implement Zero Trust principles in all IT environments, regardless of business size or vertical. Vendors of both legacy antivirus solutions and newer, behavior-based malware detection platforms have boasted that their products can detect and block as many as 99% to 99.9% of attacks. When you're confronting the sheer volume of attacks that automation facilitates, however, these detection rates are grossly inadequate.

2

WHAT YOU NEED IN AN ENDPOINT PROTECTION PLATFORM:

MULTIPLE METHODS OF DETECTING MALWARE AND FILELESS ATTACKS

Signature-based blacklisting of files can still be effective, particularly as a first layer of defense. It's quick, so it offers a method of rapidly blocking known malware. To offer significant protective value, however, blacklisting should be used in conjunction with multiple other methods of file verdicting. These include behavioral analysis, in which the file's characteristics and runtime behavior are analyzed in a decisioning environment where they can pose no threat to your systems or network. Fully accurate decisions can be reached only when expert human security analysts are available to examine the small percentage of files that require additional investigation.

Because a large number of successful ransomware attacks are executed through scripts or memory-resident artifacts that don't install any files onto the compromised endpoint, the solution should be designed to block these types of threats just as effectively as it does traditional malware files.

RANSOMWARE IS STILL ON THE RISE, AND CRIMINALS ARE BECOMING MORE AND MORE SOPHISTICATED WHEN IT COMES TO CHOOSING THEIR TARGETS.

Ransomware attacks are estimated to have cost global businesses over $11.5 billion in 2019,[5] and experts say that a business was attacked every 14 seconds at the end of 2019. It's forecast that an attack will occur once every 11 seconds by late 2020.[6] Although the FBI claims that the sheer volume of ransomware attacks is actually stable, their success rate is much higher than ever before, along with the amount of money extorted by criminals.[7]

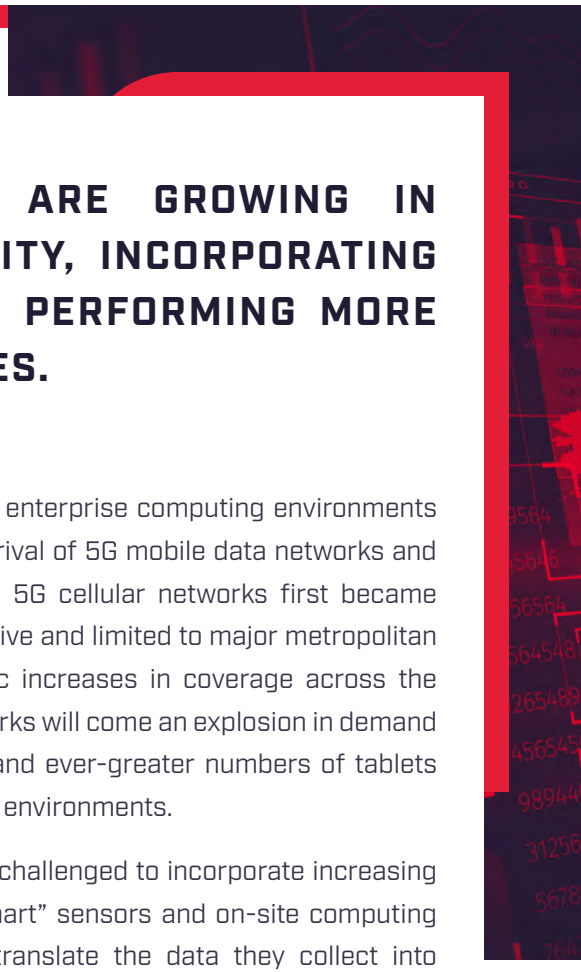
These attacks can arrive via drive-by download, through malicious email attachments, or from users clicking on infected links. Some ransomware strains target known software vulnerabilities, while others are novel zero-day exploits that wouldn't be detected by legacy signature-based anti-malware programs.

3

WHAT YOU NEED IN AN ENDPOINT PROTECTION PLATFORM:

VISIBILITY AND CONTROL ACROSS MULTIPLE DEVICE TYPES AND PLATFORMS

As enterprise computing environments evolve to incorporate an ever-broader variety of devices, look for an endpoint protection platform that supports not only Windows and OS X, but also iOS, Android, Windows Server, and Linux devices. Be sure that the solution can monitor for—and block interference with—critical operating system activities on all types of devices. And verify that application activities and system processes can be monitored from a single, easy-to-use dashboard interface across complex network environments.



ENTERPRISE NETWORKS ARE GROWING IN COMPLEXITY AND DIVERSITY, INCORPORATING MORE DEVICE TYPES AND PERFORMING MORE PROCESSING AT MORE SITES.

The two developments most likely to reshape enterprise computing environments in the early part of the new decade are the arrival of 5G mobile data networks and increasing use of edge computing. Although 5G cellular networks first became available in 2019, connectivity remains expensive and limited to major metropolitan areas. This will change in 2020, as dramatic increases in coverage across the country are on the horizon. With 5G data networks will come an explosion in demand for "bring your own device" (BYOD) support and ever-greater numbers of tablets and mobile devices connecting to corporate IT environments.

At the same time, enterprise networks will be challenged to incorporate increasing numbers of connected devices, including "smart" sensors and on-site computing devices with enough processing power to translate the data they collect into business intelligence. Taken together, these trends mean that the number of endpoints that IT departments will need to secure is poised to grow astronomically. Larger numbers of connected devices make the challenge of providing effective centralized management exponentially more complex.

4

WHAT YOU NEED IN AN ENDPOINT PROTECTION PLATFORM:

CLOUD-NATIVE ARCHITECTURE

Simply put, legacy endpoint protection tools weren't designed for today's cloud-ready digital business environments. A cloud-native architecture, in which the platform automatically and continuously updates, simplifies deployment and allows all users, across the whole of your organization, to benefit simultaneously from the very latest threat intelligence. In today's most advanced solutions, access to a cloud-based file verdicting platform means that expert human cybersecurity researchers are on hand 24x7 to examine any files that warrant this type of investigation.

BUSINESSES OF ALL SIZES ARE ACCELERATING THEIR MOVE TO THE CLOUD, BUT SECURITY INFRASTRUCTURES ARE NOT ALWAYS KEEPING PACE.

For a majority of enterprises, the journey to the cloud is proceeding at breakneck speed. The market for cloud infrastructures and services is growing three times as fast as any other branch of IT, and forecasters anticipate that this pattern will continue.[8] Still, cloud migration projects are notoriously complex, and it's not uncommon for security challenges to become a roadblock to progress.

Relatively few organizations make the leap straight to a single public cloud provider. For most, building hybrid or multi-cloud environments makes the most sense, but this "best of both worlds" approach can make maintaining control and visibility enormously challenging.

5

WHAT YOU NEED IN AN ENDPOINT PROTECTION PLATFORM:

ACCESS TO EXPERT HUMAN ANALYSTS

Look for an endpoint protection solution that incorporates the intelligence of humans as well as the efficiency of machines. Through the combination of initiating automated actions to handle the most straightforward tasks—file lookup, behavioral virus analysis, static and dynamic file investigation—and calling in expert researchers in more complex circumstances, a solution can balance speed and thoroughness in its detection procedures.

ATTACKERS' DWELL TIMES ARE LONGER THAN EVER BEFORE, AND AS A CONSEQUENCE, DATA BREACHES ARE COSTLIER.

According to the Ponemon Institute, the amount of time between the onset of a data breach and the moment of its discovery grew by 4.9% to an unprecedented 279 days in 2019.[9] As in previous years, the faster a breach can be identified and contained, the lower the costs associated with it. Yet the automated tools in use in today's IT environments do a poor job of identification and containment when their capabilities are not augmented with expert human monitoring.

7 VITAL QUESTIONS TO

ASK YOUR PROSPECTIVE VENDOR

1. Will this solution run on all the devices in my environment?
2. How long will deployment take?
3. What will the members of my team need to know or learn in order to work with this platform?
4. What types of preventative controls are in place?
5. From where does the vendor get its threat intelligence?
6. How does this solution integrate with incident response workflows? Is 24x7 professional support available from the vendor?
7. Can this solution be integrated with other security services, products, or platforms from the same vendor to reduce costs and complexity?

CONCLUSION

Endpoint security has never been more complex—or more challenging—than it is today. Given the number of vendors and solutions on the market, it can be exceedingly difficult to sort through all the competing claims to find what's truly effective.

Unlike any other solution available today, Comodo's Advanced Endpoint Protection (AEP) platform uses on patent-pending auto-containment technology, which confines unknown files and runtimes to a virtualized sandbox environment where they're not given access to host system resources or user data. It's uniquely lightweight, operating without impact on performance or end user experience. Plus, Comodo AEP was purpose-built for use in Zero Trust architectures.

Comodo's cloud-native endpoint protection technology was designed specifically to address the challenges inherent to today's complex and diverse enterprise IT environments and the sophisticated threats they confront. It includes automated file verdicting capabilities to deliver rapid results as well as access to cloud-based resources when more detailed investigations are warranted. Comodo's team of expert security analysts and threat researchers is standing by 24x7 to handle the most complex cases.

No one can be certain what the future will bring. But we're confident that the power of our technology and the scalability and flexibility of the cloud will enable us to continue detecting new and emerging attack tactics, and blocking zero-day exploits—before any of our customers suffers a breach.

COMODO
CYBERSECURITY

ABOUT COMODO CYBERSECURITY

In a world where cyber attacks are inevitable, Comodo Cybersecurity provides active breach protection with its cloud-delivered, Zero Trust platformv. The Comodo Dragon platform provides a Zero Trust security environment that verdicts 100 percent of unknown files. The platform renders an almost immediate verdict on the status of any unknown files, so it can be handled accordingly by software or human analysts. This shift from reactive to proactive is what makes Comodo Cybersecurity unique and gives them the capacity to protect your business—from network to the web to cloud—with confidence and efficacy.

Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Clifton, N.J., Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for businesses and consumers worldwide.

MAKE THE SHIFT TO ACTIVE BREACH PROTECTION

THE LEADING CLOUD-BASED CYBERSECURITY PLATFORM

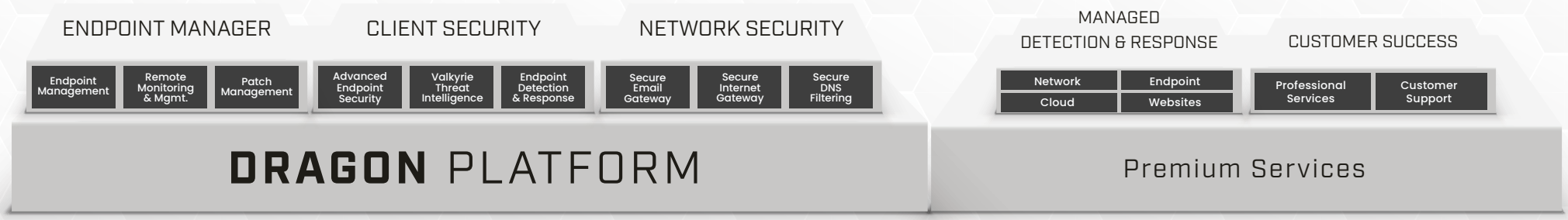
No one can stop 100% of threats entering a network, but a Zero Trust Platform can stop 100% of infections. Contact us today to set up your no obligation 30 day free trial.

COMODO CORPORATE HEADQUARTERS

1255 Broad Street, Clifton, NJ 07013 United States of America

Experienced intrusion? Contact us at 1 (888) 551-1531

Visit **comodo.com** for your free 30 day trial



ENDNOTES

1. https://blog.rapid7.com/2016/03/31/idc-says-70-of-successful-breaches-originate-on-the-endpoint/
2. https://databreachcalculator.mybluemix.net/executive-summary
3 https://www.forrester.com/report/Justify+Security+Budget+By+Its+Impact+On+Maturity/-/E-RES136453
4. https://www.wired.co.uk/article/ai-cyberattack-mike-lynch
5. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread
6. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/
7. https://www.ic3.gov/media/2019/191002.aspx
8. https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g
9. https://databreachcalculator.mybluemix.net/executive-summary