AVASANT

HCL COMMVAULT

PROTECTING THE SECURITY PERIMETER IN A COVID WORLD

Cyberattacks have been a constant threat since the dawn of the internet age. Adversaries have been increasing their attacks, whether they be nation states or financially motivated. Ironically, the same technologies that are transforming business--cloud, the internet of things, and mobile devices--are being used by hackers to exploit vulnerabilities due to inadequate configuration and controls. Now, with millions of employees working from home, IT leaders suddenly have to define a greatly expanded perimeter. This timely white paper spells out the increasing threat triggered by the sudden explosion in the number of remote workers. It highlights the key security measures that organizations of all sizes must employ to counter these threats and ensure high levels of security and privacy in the COVID world.

EMPOWERING BEYOND

www.avasant.com

AN EXPANDED SECURITY PERIMETER WITH WORK-FROM-HOME

The need for improved cybersecurity is not new. Enterprises have been targeted by cyber adversaries, whether nation-state or individual actors, for decades. Cybersecurity spending increases every year to counter the wide array of attack vectors. And for the most part, cybersecurity professionals are aware of the common patterns of these threats.

However, the Covid-19 pandemic has forced many workers out of the traditional office setting. Working from home is more prevalent than ever, our research indicates that, when the pandemic ends, the percentage of employees working 100% from home will nearly double from its pre-pandemic levels. Removing employees from the perimeter set up around the physical office has intensified nearly all of these cybersecurity challenges.

IT leaders can no longer rely on physical firewalls, company-issued hardware, and other on-premises security tools to protect enterprise data. Since the lockdown, many employees and IT staff have created ad-hoc business processes using whatever technology they had available. Their actions typically have not been malicious or incompetent, rather just an honest effort to "get the job done."

Enterprise IT organizations today have been forced to accept this state of affairs for the sake of business continuity. In many cases, IT leaders have had little lead time, with organizations going from a few dozen to a few thousand employees working from home practically overnight. And with budgets tight due to economic recession, many companies are facing multiple new cybersecurity threats with little budget to invest in new equipment or technology.

Since COVID quarantines began in March 2020, the FBI has seen a 300% increase in reported cybercrimes. Things are no different outside the US. IT organizations are simply not doing enough to mitigate security risks resulting from employees working from home. And the incentive to do better should be high. On average, share prices drop 7.2% after a data breach. Companies face lasting damage to their brands. They also risk alienating partners and other stakeholders.

THE NEW "THREATSCAPE"

The cybercrime threat is not new. What is new is that enterprises have less control over their perimeters than ever before. Employees use home networks that employers have no control over, misconfigured routers, unpatched firmware, or default passwords. They may be transmitted confidential data over public Wi-Fi. Next generation technologies like the cloud, IoT, and mobile devices are transforming enterprises and enabling them to work from home. However, this technology also allows hackers to exploit vulnerabilities due to inadequate configuration and controls.

It isn't just the employees, but the technology itself that can carry risks. The cloud is an example. There's a frequent misunderstanding between the cloud provider and the customer. There needs to be a clear

shared responsibility model agreed upon with the provider. Who is securing the data? Who is controlling the levers of security? But too often, these responsibilities are not spelled out, or they need to be addressed in light of the current crisis. We're facing undeniable cybersecurity risks throughout industry that lead to negative consequences if left unaddressed.

Combine the threat landscape with the move to mobile technologies, the cloud, and the need to work from home, and you have a dangerous and fast-changing environment that can challenge any organization.

Business and IT leaders need to recognize the two main categories of cyberthreat actors. The first is the criminal. Cybercrime will never go away as long as the financial rewards are so high. Noted bank robber Willie Sutton was once asked why he robbed banks. And he is quoted (likely erroneously) as having said, "That's where the money is." Sutton's law as used in cybersecurity, medicine, and several other fields basically means we shouldn't ignore the obvious cause for things. Why will criminals target your enterprise for data? Because your data is valuable.

Ransomware is the primary activity utilized by criminal organizations. And traditional mitigations used to thwart ransomware attacks are becoming obsolete. Companies need to consider air-gapping and reducing network exposure for critical data, completely disconnecting backup storage devices from networks to mitigate the risk of backup data corruption.

The second major category of cyberthreat actors is nation-state actors, which account for a majority of data breaches. Their motives are not as readily apparent, but several recent high-profile data breaches, such as those targeting COVID-19-related research firms and national elections, have been leveled by nation-states against their geopolitical adversaries, large corporations, and specific industry sectors.

The Cybersecurity Glass Is Half Full

Cybersecurity during these times of crisis is not a lost cause. There are countermeasures available and ready to be leveraged. The empty half of the water glass tells us that skilled security professionals are scarce and that security processes are oftentimes lacking. The full half of that same glass is filled with security technologies available, developed by providers teaming with innovation and a forward-leaning vision.

So what is a company to do in light of this new portfolio of technology, a new perimeter to protect, and an increasingly global threatscape?

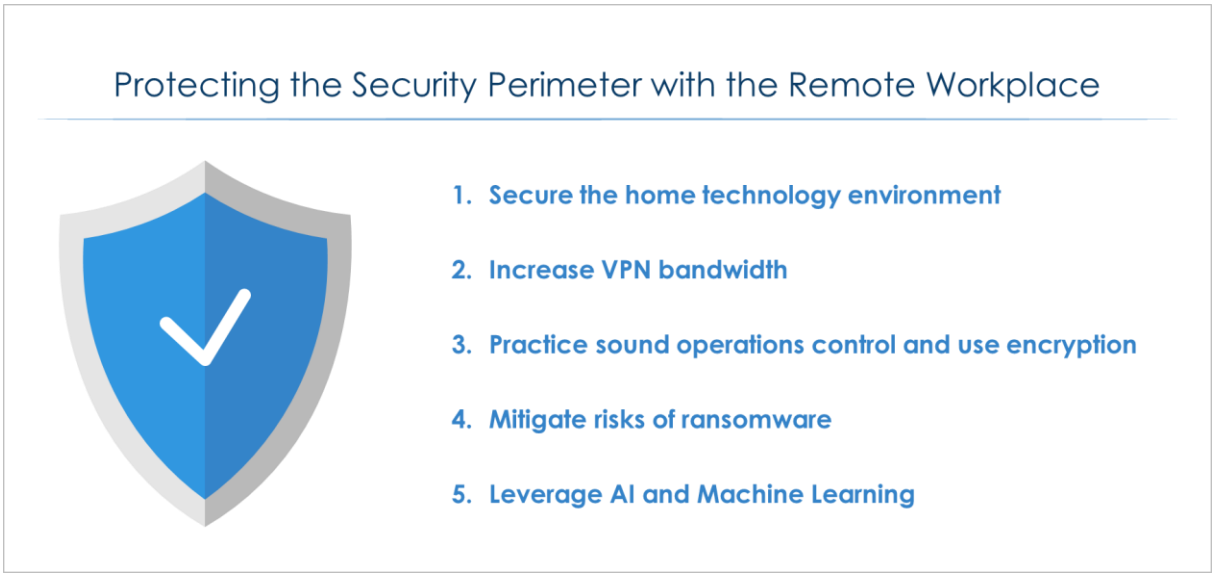
First, every organization must focus on the people-side of the equation. This means having someone, or more likely a small group of security professionals, with the responsibility and authority to formulate and enforce security policies, procedures, and controls, and making them an integral part of business processes. It also means increasing the security awareness of the entire workforce. At the same time,

security service providers can provide needed skills that may be lacking within the enterprise, especially when those skills are in short supply.

As noted, technology can be brought to bear on the problem. Use of artificial intelligence and machine learning can be leveraged to automate routine security activities, such as log monitoring, letting security specialists focus on higher value-added security responsibilities.

Also, as a precursor to any major change in security technology or processes, companies need to manage the basics: OS updates, security patches, antivirus signatures – all must be kept current. There's no way to proceed if the simple controls aren't established and maintained.

With these principles in mind, here are five practical recommendations for protecting the security perimeter in the COVID world:



1. **Secure the home technology environment.** At home, employees may have their guard down about simple security practices. The fact that they might be working in their pajamas or their kids might be nearby may cause a loss of focus. As noted earlier, their home equipment may not be adequately secured. Within bounds of privacy, help workers lock down their home networks. Retrain them on potential phishing scams. Help them separate work data and personal data. Where appropriate, implement two-factor authentication, single sign-on, and other access controls. Most of all, when possible provide work equipment for work. Don't rely on the technology choices of your employees now that we've reached a new normal of working from home.

2. **Increase VPN bandwidth.** VPNs are vital for home workers. But VPN bandwidth may not be sufficient to handle a several-fold increase in the number of employees working remotely. Not only does VPN bandwidth need to be sufficient to handle SaaS applications and the digital workspace, but it also needs to be configured for individual needs when circumstances warrant.

While improving your VPN infrastructure, be sure the VPNs and the applications used on them are regularly updated and patched.

3. **Practice sound operations control and use encryption.** Employees making use of ad hoc business processes, data storage, and personal hardware are likely introducing vulnerabilities. Do not permit the use of thumb drives to move data from office to home, and when possible, disable USB ports. Do not allow for the use of personal online storage such as DropBox (unless using an enterprise license with appropriate controls). Encryption is also vital both while data is at rest and in transit. You should seek to understand your environment and exactly how large your perimeter is based on your cloud footprint, SaaS-based solutions, employee-owned devices, and social media presence. Maintain controls over the entire footprint.

4. **Mitigate risks of ransomware.** Ransomware is not only one of the most common threats but one of the most crippling. If you find your data encrypted or stolen, mitigating the loss is key. Because cybercriminals often corrupt data over many months, review your backup retention schedule to ensure you can get back to an uncorrupted backup. Backups with reduced network exposure or even "air gapped" backups, as noted earlier, may allow you to restore most or all of your missing data. By storing backups either off network, on a different network, or at least limiting network exposure, you can often restore some or all of the data being ransomed. There are tradeoffs to consider including the cost of the system, the gap in time between backups (which equates to how much data is lost in a given attack), the speed of recovery, and the ease of recovery. However, mitigating against this type of attack is essential.

5. **Leverage AI and Machine Learning.** As mentioned previously, some traditional mitigation strategies are no longer viable. AI and machine learning can help level the playing field. AI can monitor inbound and outbound data for unusual patterns, simultaneous or geographically unlikely log-ins, and unusual or excessive data requests, all at the speed no human can replicate. ML can identify likely phishing scams and constantly scan the landscape for potential threats. Most of all, while AI can't replace the need for well-trained security personnel, it can augment their capabilities and reduce the dependence on people. As stated above, there is a shortage of security talent. AI, combined with a judicious use of service providers can mitigate the lack of talent and identify threats quicker.

Weathering the Perfect Storm

As companies seek mitigations and solutions to this perilous threatscape, the often-used cycle of people, process, and technology must be considered. The lack of qualified human resources and fragmented processes and policies leads many to consider technology-based solutions. When doing so, company-specific risk assessments should lead to the right solution. It's difficult to imagine, for example, that ransomware wouldn't be a priority risk for all organizations.

Companies should be operating in the cycle of verification, validation, and consideration as it relates to testing their resiliency against ransomware. Does your toolset offer this? What about business continuity and disaster recovery? How quickly can you recover lost or corrupted data? How safe is your backup data? Can you air-gap the backup data? Most network environments house multiple platforms, data types, and APIs. So, scalability is key in the planning stages. When addressing the technology piece of the stated cycle, data management allows for these protections and ensures a calm, measured response in times of stress (i.e. data loss, data deletion, all-around bad hacker-sourced disasters, etc.). Data management is more than a tool – it's a program that provides multiple solutions and should be strongly considered in any information security strategy.

Today's rapidly changing environment has evolved the traditional view of an enterprise's landscape into that of a threatscape. A perfect storm is among us in the sense that we're expediting a transition to the cloud while defending ourselves from cyber criminals. But the new x-factor is the global pandemic. Enterprise IT organizations have suddenly found themselves stripped of on-premises security weapons. The perimeter they've been asked to secure has suddenly been enlarged and without their design or impetus.

It can be overwhelming to address this evolving threatscape with certainty. But, understand that lifesavers do exist. Picking the right ones is important and can be accomplished with awareness and research. Remember – if it's predictable; it's *somewhat* avoidable and at minimum - recoverable. Criminal activity and data targeting is predictable. We've been given the data to make informed decisions. The least we all can do is be prepared.

About the Author

John Caruthers is a Fellow at Avasant, Director, Illumina and Former Supervisory Special Agent, FBI. For more information, please contact him at john.caruthers@avasant.com or learn more via https://avasant.com/team/john-caruthers/.

About Avasant

Avasant is a leading management consulting firm focused on translating the power of technology into realizable business strategies. Specializing in digital and IT transformation, sourcing advisory, global strategy, and governance services, Avasant prides itself on delivering high -value engagements through industry focused innovation and flexible client based solutions.

Email – contactus@avasant.com | Phone - +1 310 643 3030 | Visit us at - www.avasant.com