COVID-19 and beyond: Will the work-from-home explosion revolutionize enterprise security architecture?

Analysts - Scott Crawford, Daniel Kennedy, Fernando Montenegro, Eric Hanselman, Garrett Bekker, Aaron Sherrill

Publication date: Thursday, April 2 2020

Introduction

In previous spotlights, we have looked at the explosion in work-from-home (WFH) initiatives driven by the global coronavirus outbreak and the surge in demand for secure remote access that they require. This shift, like the pandemic driving it, is like nothing ever seen before. It is disruptive in ways many organizations had not dreamed possible. And disruption is the antithesis of a well-ordered approach to security on which many organizational strategies are based – which raises the bar for defense and introduces opportunity for adversaries.

The 451 Take

In our last spotlight on this subject, we discussed some of the technologies that organizations will use to secure this access, both to meet immediate need as well as for more lasting, longer-term access to a variety of resources in the cloud as well as in the enterprise datacenter.

But what about assuring security once that access is provided? Organizations will need to prepare for opportunistic attacks seeking to take advantage of vulnerabilities. They will need to monitor IT use for evidence of malicious behavior, protect sensitive data and assure compliance with privacy and other regulatory requirements. And in a world where cloud concepts increasingly dominate, with multiple hosted services providing functionality previously owned and operated by on-premises IT, many existing approaches to solving these problems predicated on deployment within a traditional enterprise network are now showing their age. We expect that the WFH boom created by the COVID-19 pandemic will spark initiatives to modernize enterprise security. Perhaps not in the next few months as organizations scramble to meet immediate demand, but as WFH becomes more entrenched, it will almost certainly catalyze long-term investment in such initiatives.

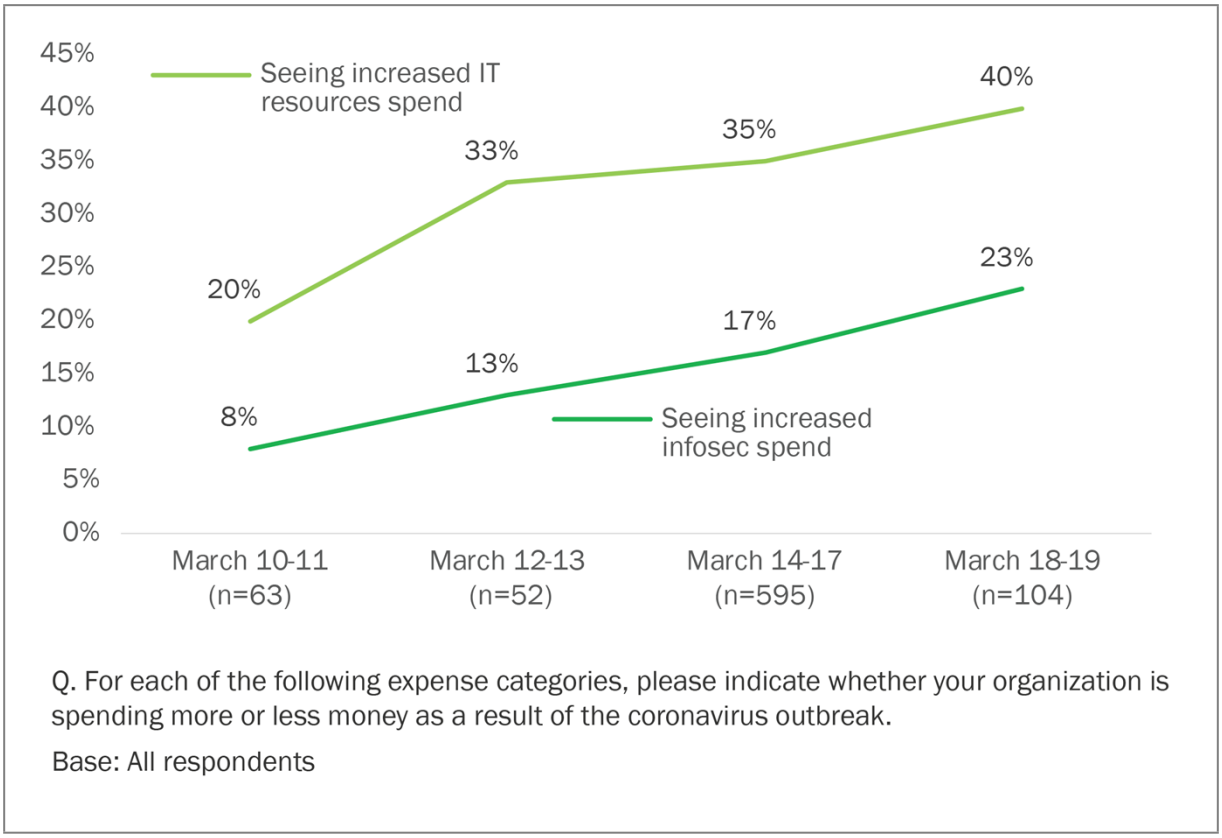
Initial fallout: Opportunistic attacks and spending to adjust to the new reality

One of the first things beyond access that organizations must be aware of is the invitation to adversaries that such massive disruption introduces. Already, opportunistic attackers have sought to capitalize on the coronavirus outbreak in multiple ways. Phishing attacks, the second most cited pain point in 451 Research's end-user studies, are targeting employees scrambling to cope with new and unfamiliar ways to access enterprise resources. Attacks invite them to click on guidance, download new network configurations and other enticements to execute malicious content in messages. The unscrupulous targeting those in greatest need in a suddenly uncertain economy are preying upon expectations of support such as government assistance, directing the unsuspecting to malicious sites where victims will supposedly receive direction on accessing disbursements or guidance on handling money transfers. Some attackers have sunk to targeting overstretched hospitals with ransomware, as happened to Brno University Hospital in the Czech Republic in mid-March.

The users of virtual collaboration platforms aren't immune. In recent days, malicious parties have 'crashed' accessible online meeting venues to disrupt virtual gatherings of those seeking to remain productive and in contact with each other, as hosts scramble to learn new platforms and configure their meetings to prevent such intrusion. Trojaned versions of collaboration platform applications have appeared, while platform providers have hastened to address security and privacy concerns arising from their increased visibility and use.

Already, providers of security awareness training, anti-phishing, email security and other domains are stepping up their efforts to increase this awareness and improve individual response to such attacks. But this is just one aspect of the challenges organizations face at the point where people interact with technology and they have ramped up their spending plans accordingly in just the last few days.

Figure 1: More Organizations Project an Increase in Infosec Spending as the Crisis Worsens



Source: 451 Research, Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey March 2020

Moreover, enterprises are seeing that this increased investment will have a long-term impact beyond the immediate crisis:

"Let's call it, 1,200 people that are working from home, and you're spending like $1,200 on a laptop, you're at $1.5 million right there. You can't buy that and just keep paying for empty offices, electric, heating, cooling, parking. And [maybe] you're in a town where real estate is very expensive anyway. So I could see very easily that kind of flowing throughout the community, and a lot of people saying, 'Hey, we went home for the coronavirus. We stayed and we're more productive.'"

-IT Engineering Manager/Staff, 1,000-1,999 employees, $100-249.99m revenue, Health Care

Source: 451 Research's Voice of the Enterprise: Workloads and Key Projects 2020

When it comes to security, where are these investments are likely to be focused? Let's start with the often newly remote users themselves and their personal devices.

In the remote environment: endpoints and local networks

Securing a corporate endpoint is challenging enough within the traditional enterprise network. Now that those endpoints may be on any network outside the organization, making sure that each one has current security protections, with patches installed and an up-to-date and secure configuration, is an even greater challenge. Endpoints may not be continuously accessible or may be on lower-bandwidth network connections. Organizations that must rely on the skills and diligence of individual users are at a clear disadvantage in keeping these endpoints protected against exploits.

Some organizations may have switched to supporting user-provided endpoints – the traditional BYOD approach. In those scenarios, there's a multitude of issues to consider, including non-

controlled software installations, compatibility issues or shared access considerations, and whether and how much organizational management control will be tolerated by employees on personally owned devices. For the enterprise, the dilemma is further exacerbated by a long-standing concern for endpoint management: how many endpoint agents are too many? Downward pressure on this number is clearly evident in 451 Research Voice of the Enterprise data that shows the number of endpoint security products falling on average from 3 to 2.6 over the last two years, with 62% of respondents to our 2019 Voice of the Enterprise: Information Security, Workloads and Key Projects study reporting no new endpoint security products implemented in the previous 12 months.

The local networks to which these endpoints connect may present an even bigger concern. Home Wi-Fi may not be configured safely enough to prevent neighbors from eavesdropping on local connections and is less likely to be updated with the latest firmware. As we've seen with the recent Kr00k vulnerabilities, even enterprises are having a difficult time updating when a critical vulnerability is revealed. One mitigation is to use virtual private networks (VPNs) to reduce eavesdropping risk, but that adds strain to already burdened VPN capacity. Within the home network, a variety of devices may connect to multiple consumer services with varying degrees of protection and control. These devices may, in turn, connect with endpoints used in the enterprise – with potential for exposing sensitive data or functionality in the process. There are even monitoring considerations, as security operations centers (SOCs) may note activity from these remote devices that analysts are not used to seeing in traditional office networks.

VPN: One size does not fit all

Securing these endpoints from these threats may raise the bar on the nature of endpoint protection. Securing a sensitive network connection all the way to the endpoint and limiting its exposure, even on the local home network, will likely become a higher priority once organizations solve their most immediate remote access needs.

Virtual desktop infrastructure (VDI) is one approach that can deliver a corporate endpoint experience under strict enterprise control, with benefits that could extend far into the future. For broader access, however, many are relying on the most basic technique to isolate enterprise functionality in the field: the VPN. Extending VPN to new users and use cases helps solve some immediate problems of isolation and segmentation. It also comes under immediate pressure, as organizations see VPN access capacity straining under a scale of remote work until now unforeseen. At least if the endpoint is on the VPN, that is a network known to the enterprise and access can be segregated at least on that basis, if nothing else. But for every gain there are also losses.

For one, VPN-connected endpoints may all find themselves on effectively the same network – a network that may be necessarily flat and relatively unsegmented so as not to interfere with critical access to target resources. The network context from which a user connects may not be as granular as in the traditional enterprise, where access can be segmented based on local subnet or other logical topology – which also helps to limit the spread of malicious activity, if it can be confined to specific subnets. This points up an Achilles' heel of many legacy security policy premises: segmenting access based on network host address or network of origin may no longer be enough to establish whether the endpoint and its user should be granted the access it seeks.

This is part and parcel of the move toward 'zero trust' initiatives that predicate access more on multiple demonstrable assets of the user, the endpoint, the target and the nature of access sought. Up until the current crisis, it was generally accepted within industry that 'zero trust' had two key initial use cases: secure remote access for a relatively well-defined mobile workforce and microsegmentation of datacenter traffic. No one expected that for many organizations, the mobile workforce would suddenly be nearly synonymous with the organization itself.

Beyond connection: maintaining visibility and control

One of the most significant reasons VPN remains so important, however, has nothing to do with access per se. It is mainly because traditional approaches to enterprise security monitoring and control depend on visibility within the traditional enterprise network, where organizations can deploy the instrumentation required to see activity, apply analytics to identify anomalies and impose control to limit malicious behavior when discovered.

How does the nature of that visibility change when workers move beyond the enterprise network? Consider, for example, that access to a given resource may appear to be an anomaly when multiple access attempts are made from an off-premises network, when that user previously accessed a target only from inside a company building. Hundreds of users coming in through the same VPN concentration point may be undifferentiated in how they access the network, which reduces the value of context unless additional attributes are assessed. It's not unheard-of for users to share a login to gain access to a resource critical to many at times like these, but ordinarily restricted to a single user account. Identifying such anomalies may be key to refining privilege management to meet emerging needs.

Monitoring and visibility will have to adapt not only to a workforce that is more distributed, but to resources distributed among a growing number of third-party and cloud services as well. The enterprise has evolved beyond home-grown IT – but security monitoring often has not.

People are distributed – but resources are now, too

Visibility and control concentrated on the traditional on-premises enterprise network is in direct opposition to trends reshaping the nature of enterprise IT. Increased reliance on third-party cloud, hosted services and SaaS means that enterprise users can access these resources from anywhere – and these resources can be found virtually everywhere. When control over enterprise policy for accessing and interacting with these services is not an issue, why would users need – or even want – to tunnel back to the enterprise network, in order to tunnel back out again to third-party resources that may perform far better when connected directly, with as little as possible between the end user and the target?

This is the one of the single biggest issues weighing down the future of enterprise cybersecurity. So much is now delivered from the cloud by third parties that forcing traffic back through a legacy enterprise network looks increasingly like an anachronism. But how can organizations preserve the visibility and control they need? How will they know when individual users, vital functionality or sensitive resources have been targeted – and how can they protect those users and resources with the expertise that individuals cannot and should not be expected to wield themselves? How can organizations protect their interests, when their third-party providers may have little or no responsibility for a breach for which the enterprise is ultimately responsible?

It seems inevitable that emerging tactics will need to preserve this visibility by interposing into interactions between end users and target resources in some meaningful way – but dragging traffic back to a VPN concentration point will likely not be the preferred method indefinitely, if only for availability and capacity considerations alone. Some approaches may seek to deliver this functionality via cloud-based providers with multiple geographic points of presence that map well to the availability of the target resource. The performance of these services will have to meet or exceed that expected from direct connection to the target – which makes it seem likely that cloud providers in the best position to meet this demand may either embrace these trends directly or become key enablers of new approaches.

This is the realm of the emerging secure access service edge (SASE) – but as with 'zero trust,' SASE so far is more of a large-scale trend that embraces multiple segments of technology to facilitate this sea

change in the nature of distributed enterprise security. As we described in our previous report, many contributing segments range from cloud access security brokers (CASB) for SaaS applications to software-defined perimeter (SDP) approaches and wide area networks (SD-WAN).

But how will monitoring and visibility plays capitalize on these trends? Vendors in relevant segments must still bring together information from all these sources to synthesize actionable insight for security teams and to facilitate effective response. In some cases, we expect the providers of these distributed security services to deliver or concentrate insight themselves. But will a collection of players across multiple segments be able to consolidate the comprehensive visibility that enterprise security teams need to act? It seems likely that those with the most to lose in such a trend – those whose play has primarily been predicated on deployment within the enterprise network – would be most incented to concentrate this visibility and preserve the upper hand among a collection of tactical approaches to distributed control.

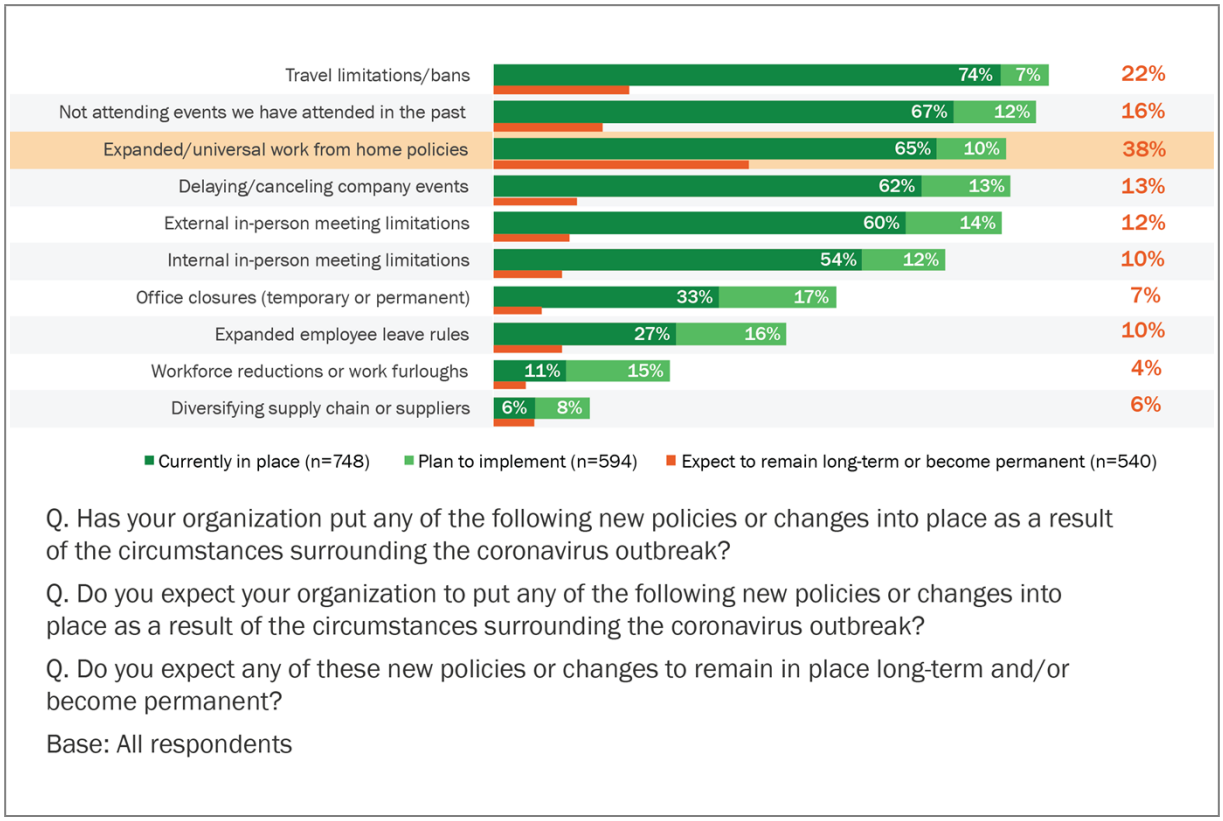
And what about the target resources themselves? Not every cloud computing deployment is amenable to having yet another security measure bolted onto the front door to protect access and assure secure interaction. Each provider's embrace may differ, just as the deployment models for IT in the cloud vary from platform to platform, application to application, and between infrastructure-as-a-service models to SaaS.

This movement toward newer visibility options should further accelerate the transformation implied by two of 451 Research's major modern paradigms: Invisible Infrastructure and Universal Risk. In a world where the infrastructure details fade from the customer's view, organizations are going to need a much more sophisticated and nuanced perspective of what risk actually is. Over time, we expect much more attention to higher-level concepts within security teams, away from infrastructure and more toward application and business-level considerations.

We won't be going back

Regardless of which direction security takes to navigate through the current crisis, a significant number of respondents to our recent 451 Research Voice of the Enterprise Digital Pulse flash survey (38%) believe that working from home will likely be long-term or permanent.

Figure 2: Organizational Policy Response to the COVID-19 Pandemic



Source: 451 Research, Voice of the Enterprise: Digital Pulse, Coronavirus Flash Survey March 2020

It therefore seems likely that the current crisis may light a fire under these new security models like nothing before. Gaps that the haste to enable large-scale remote work will open will have to be closed – some sooner than others, and not all such fixes may be permanent. But if an outcome of the current crisis is a more enduring entrenchment of remote work for the indefinite future, the changes in enterprise security architecture they precipitate may come to stay.