WHITE PAPER

OUTSOURCING SECURITY OVERCOMES COVID-19 PANDEMIC CHALLENGES

No organization wants to suffer a security incident or make headlines due to a data breach. Malicious hackers can steal confidential company data or take down everything from critical systems to the whole enterprise. However, in recent years new threats and increasingly sophisticated cyber-criminals have made it more difficult than ever to maintain an adequate defense.

Now, enterprise IT professionals are being hit with a one-two punch. On top of growing threats, they must also support employees – or in some cases an entire company – displaced by fears of contracting COVID-19 in the work-place or from commuting on public transportation.

It seems that almost overnight the current global pandemic has essentially transformed many organizations into virtual enterprises. From Silicon Valley to the valleys of New York's financial district, many headquarters buildings stand vacant as employees work from home. Even when the pandemic abates, many of these workers may never return to working on-site on a full-time basis. Which means protecting remote employees' devices and the networks that connect them will, for the foreseeable future, continue to present huge hurdles for IT leaders and cybersecurity professionals.

In addition, as more companies strive for digital transformation, there is simply more data to steal and more systems to attack. IT organizations also continue to move core business compute functions from the conventional data center to cloud and multi-cloud environments. And as data and computing moves to the edge, the proliferation of mobile and IoT devices make protecting endpoints a more daunting task.

FAILURE TO PROTECT THE NETWORK IS NOT AN OPTION

Consequently, IT teams must adapt their data, network and security strategies to cope with this sudden increase in demand for remote access to data and core business applications. The good news is these teams have leveraged cloud-based applications and networking technology to effectively support remote operations.

At first, this comprised an emergency effort to ensure business continuity. However, as a significant percentage of many companies' workforces are social distancing at home, it becomes critical to focus on securing this new normal. This is especially true when you consider the risks that come from the many remote devices, SaaS apps, and collaboration technologies.

Technologies such as video conferencing and remote file sharing also present unique security challenges.

Failure to secure all these devices and tools – as well as the network access needed to support them – risks incurring significant hard and soft costs. For example, in the event cybercriminals make off with customers' personally identifiable information (PII), the legal and regulatory responses can distract the organization for years.

On top of these risks, organizations can incur soft costs such as brand damage and managers having to focus on legal and regulatory issues rather than business. For instance, few have forgotten the devastating breach that impacted Equifax. In its first-ever action related to a cybersecurity incident, ratings company Moody's downgraded Equifax based partly on costs that included a $690 million charge in a single quarter resulting from ongoing class actions and regulatory fines. And those hard costs do not include the hit a brand can take after making mandatory public disclosure of a security incident required by privacy laws such as California's SB1386.

https://www.forbes.com/sites/kateoflahertyuk/

Plus, at a time when many companies are facing lower revenue, few can afford the high cost of breach remediation. According to a recent study by Juniper Research, the cost of data breaches will rise from $3 trillion annually to over $5 trillion in 2024, or an average annual growth of 11%. To further exacerbate the challenge, lower revenue is also translating into fewer dollars available for security.

That said, throwing money at the problem would not necessarily represent a realistic solution. IT leaders have struggled for years with a shortage of security experts, and it is not getting better.

Speaking at a recent TechCrunch conference, Jeanette Manfra, assistant director for cybersecurity at the Department of Homeland Security's Cybersecurity and Infrastructure Security (CISA), said: "It's a national security risk that we don't have the talent, regardless of whether it's in the government or the private sector. We have a massive shortage that is expected to grow larger."

NEW NORMAL, NEW CHALLENGES

Given this dramatically transformed IT landscape, your teams may face a number of chronic security challenges as well as new ones, including:

- Overly complex security stacks
- Vulnerabilities that remain unpatched for months due to shortage of skilled security professionals
- Service desks being crippled by surges in tickets, including COVID-19-themed malware incidents
- Difficulty retaining security analysts after you have trained them on your environment
- A lack of in-house expertise in various aspects of compliance
- Too many alerts, which can lead to alert fatigue and cause threats to be missed
- Lack of visibility into remote devices needed to ensure security and compliance

In addition, while traditional EDR (endpoint detection and response) services do an adequate job of detecting and responding to single exploits on endpoints, they fail miserably when it comes to more sophisticated and distributed attacks. This is because they don't have an end-to-end, holistic view of network traffic. They also come up short on the critical human component. Consequently, these relatively expensive solutions provide little value in the face of today's threats.

XDR – BETTER BUT NOT EASY

For already short-staffed and overtaxed security teams, this results in problems such as more than half of threats being overlooked, or threats persisting for too long in your environment. A better option is XDR, a new approach to threat detection and response where X stands for the "extended" – the coming together of cloud, user, endpoint and network information.

XDR offers better protection than the typical approaches that provide only limited and isolated visibility into attacks, which results in a higher volume of alerts than most teams can handle.

The COVID-19 pandemic has taken the need for managed XDR to a new level. Understanding the security landscape with a well-defined perimeter is tough. By pushing millions of workers into home offices, the pandemic has, significantly changed the WAN, because every employee's home is now part of the network. This increases the attack surface, creating more entry points and vulnerabilities.

Nonetheless, this layered visibility can lead to problems, including:

- Too many alerts to handle
- Alerts that lack the context necessary for an effective response
- Lack of guidance, meaning investigations require analysts with specialized expertise
- An overemphasis on tools to the detriment of providing real protection for the business
- Security teams having to spend time maintaining and managing security tools rather than performing security investigations

The end result for stretched-to-the-limit security teams can include unmanageable streams of events, disjointed tools and information to pivot between, longer detection time, and security wasted budgets.

While layered visibility provides important information, it can also lead to problems. For one, the task of analyzing, correlating and visualizing the sheer volume of data generated by XDR systems can overwhelm already over-taxed security teams.

OUTSOURCING DETECTION AND RESPONSE OFFERS A REALISTIC SOLUTION TO THE COVID-19 CHALLENGE

What is the right solution and how can you improve your security quickly enough to keep pace with your newly remote workforce? By outsourcing XDR and the security operations center (SOC) to a leading security and networking provider, organizations can quickly overcome many of the challenges associated with supporting workers displaced by the pandemic. In particular, a Managed Detection and Response (MDR) solution such as the one offered by Open Systems addresses problems like the chronic shortage of security professions.

And since Open Systems also offers a secure access service edge, or SASE (pronounced "sassy"), its MDR solution coordinates the SOC with the entire SASE stack. This includes everything from the WAN to firewalls to all the network. This security network architecture provides much greater visibility into the entire cyber kill chain. The Open Systems MDR service certainly provides significant inherent value. But when combined with the SASE network, it offers greater visibility across the entire kill chain including remote locations, WANs, clouds, and endpoints.

Moreover, it combines human know-how, advanced automated threat detection, and the best sensor technology. It incorporates a cloud-scale SIEM built on Microsoft Azure Sentinel, which ensures smooth logfile integration from your existing security controls and other sources of relevant data. Logs coming in from the SASE stack further provide context that is critical for running threats to ground and providing customers with the best guidance for and effective response – before damage is done.

More importantly, it critically augments security tools with the human element. The managed SOC, which is staffed by seasoned security experts, including the DevSecOps engineers who designed it, ensure that there are always eyes on the network. These experts have an intimate understanding of each customer's environment. This continuous monitoring makes it possible to detect and contain threats as fast as possible. Furthermore, since these experts not only run credible threats to ground, but also offer guidance for response, it acts as a force multiplier for your Incident Response team.

Finally, Open Systems XDR provides network visibility, a comprehensive detection and response solution that overcomes the many challenges of securely supporting the huge surge of remote workers resulting from COVID-19 stay-at-home orders.