MARKET BRIEF

CRITICAL FUNCTIONS IN CYBERSECURITY TO PROTECT THE ENTERPRISE

You need a license to drive a car on public roads. You need a license to go fishing in public lakes and streams. You need a license to own a gun. But you don't need any kind of license to communicate on the public Internet. No accountability. Complete anonymity. It's literally the only thing you can do with public resources that doesn't require registration or a license.

Anonymity can give others a license to do all manner of awful things. This market brief explores some recent cyber attacks and critical cybersecurity functionality that IT leaders should consider when evaluating vulnerabilities within their own environment.

Advantage

ANYBODY HAVE $70 BILLION LYING AROUND?

The recent attacks on the Colonial Oil Pipeline and SBS Meat Processing are two high-end examples of what this anonymity can cost. More recently, the attack on network monitor Kaseya brought the largest ransom demand ever, some $70 Million in bitcoin.

Ransomware attacks typically start by exposing another human behavior – trust. While "trust" is arguably and, for the most part, a good thing trust can be ill-conceived when those asking for your trust are anonymous.

Ransomware attacks, which have been the most prevalent type of cyberattack for several years, begin with a "phishing" email. Users receive an email that looks very genuine, like it really comes from their bank, or a law firm, the government, or some company. The logo looks real. The typefaces are the same, as are the colors. The clues that give away the fact that they are suspicious are difficult to spot.

The email invites the user to click on a link or open an attachment. When they do, the malicious code in those links and attachments allow the cybercriminals who sent the email to penetrate every layer of data and network security their company has invested so much into. They've bypassed the user multi-factor authentication (MFA) and authorization process, zipped right past the intrusion prevention system (IPS), skipped the anti-virus and anti-malware filters and tunneled right through the firewall. All because an authorized user shared their access by clicking that link or opening an attachment.

Once inside they encrypt the data stored in data repositories making it completely unavailable to the owners of that data and leaving the owner with very few options to access their data again.

And because the Internet was designed without accountability in mind, they have no idea who's holding them for ransom. What they do know is that their business is significantly impacted in terms of computer operations. Either the company decides to pay the ransom, or they incur the time, expense, and effort to recover from the attack on their own.

MUST-HAVES TO KEEP YOU AHEAD OF THE ANONYMOUS ATTACKERS

Cyberattacks carve a path through your network defenses, so let's follow that path from beginning to end to see how we could have stopped them!

USERS

The first line of defense makes sure that the user is who they say they are. Once that's confirmed the network will know exactly which resources they are authorized to use. An ID and password are the most obvious "must-haves" here, but time and experience have proven that this is not enough. It is estimated that 80% of users use the word "password" as their password, or their spouse's name, their pet's name, "123456" of some number series like that, or "abcdefg".

Multi-factor authentication (MFA) is a "must have" in terms of cyber defense. With MFA, a user entering their ID and password is sent a secret code using their mobile device or something similar. They must enter this code before they can access the network. This combines something they know, their password, with something they have, their device.

ENDPOINT DEVICES

Everything that connects to the network at the edge is called an endpoint, and these are the likeliest point of entry for most kinds of attacks. These devices can be anything from SD-WAN devices to firewalls and any other devices that has a direct connection to a public network.

INTRUSION PREVENTION SYSTEMS

As data packets approach your network location coming from another, the IPS inspects their pattern and content to determine if they are legitimate and can be allowed to proceed to or through your firewall. For any company looking to protect their corporate assets, IPS is becoming more of a "must have".

> According to IBM and the Ponemon Institute's 2020 "Cost of a Data Breach" report, the average total cost of cybersecurity breaches in the United States of America, between August 2019 and April 2020, was $8,640,000.

ANTI-MALWARE/VIRUS/SPAM

Each of these and several other related systems are filters that check the patterns and signatures to see if data entering your network may contain any of the known variants of malware. To be effective, these engines must be updated regularly with new "signatures", of malware to be on the lookout for – a definite "must have" for all companies.

ENCRYPTION

Perhaps our best line of defense for data security. Encryption uses an algorithm to scramble your data in such a way that it can only be unscrambled by anyone who has the appropriate encryption key.

All data must be encrypted when it is in transit from one network location to another, and when it is at rest on any given storage device. For a comprehensive security solution, encryption is another "must have".

FIREWALL

Several years ago, the firewall was "gatekeeper" for all network traffic entering a corporate environment. In today's world, it is just one of the many levels of defense used to enforce your security policies by blocking unauthorized traffic according to your security policies and rules. Of course that means it's useless if you don't have a set of fully updated and maintained security policies. The firewall is one of several key components to block malware from entering your corporate systems. It is the combination and orchestration of the firewall, SD-WAN, IPS, anti-malware and other systems that make up the total security system. All must work together to be successful in thwarting cyber-attacks.

WHEN TO START?

Now. Yesterday, if possible.

If all of this has left you with the feeling there's an awful lot involved in data and network security - you're right. The freedom criminals have, in large part due to their anonymity, is often very difficult to overcome and attack methodologies are changing literally every day. Finding the right combination and level of security prevention is key. Finding the right security system and the right providers to effectively manage your security posture is critical. A failed security system has far reaching business impact in terms of data breaches, outages, ransom payments and perhaps most importantly the long-term damage to the business brand.

The most important takeaway from this tour is that you need resources to plan, design, implement, and manage your data and network security measures. It's not something that can be handled casually or after the fact. If you don't have d the resources in-house, it's important to obtain the proper expertise to understand the array of cyber threats specific to your organization and onboard the proper tools and protocols to thwart such efforts from nefarious actors.

> The reality of security today is that security leaders have too many tools. Gartner found, in the 2020 CISO Effectiveness Survey, that 78% of CISOs have 16 or more tools in their cybersecurity vendor portfolio; 12% have 46 or more. Too many security vendors results in complex security operations and increased security headcount.
>
> Gartner

Why Advantage?

We optimize the technology lifecycle

Advantage is a managed service provider that drives value to your organization through five key stages in the technology journey. Employing expert practitioners, efficient processes, and a unique software platform, we solve the challenges of managing technology in the modern enterprise.

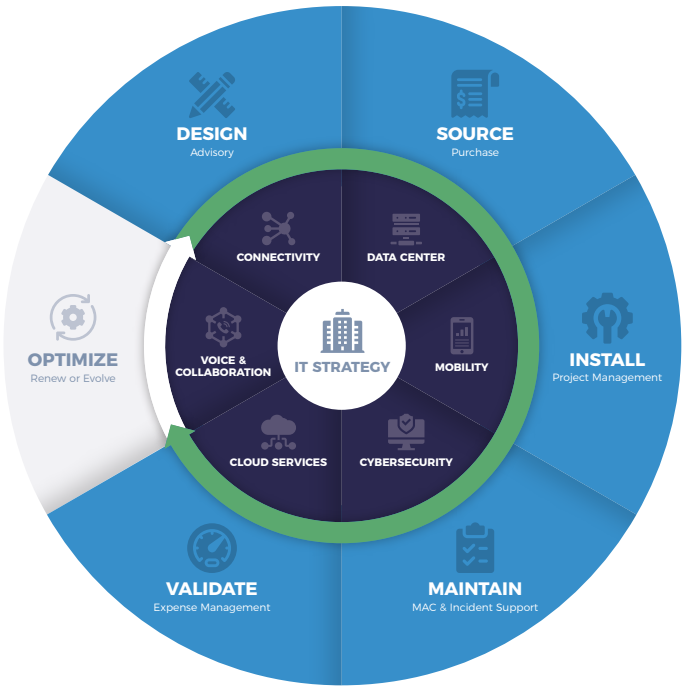
DESIGN
Based on your business drivers and global best practices, we create purpose-built solutions leveraging leading technologies and ideal providers.

SOURCE
Leverage our experience, benchmarking, and global partner network to select service providers, negotiate the best possible terms, and contract for the lowest rates.

INSTALL
Capitalize on our project management leadership for a seamless rollout of new solutions and the timely disconnect of legacy services.

MAINTAIN
Ongoing managed support of daily activities such as moves, adds and changes to your services, while having full visibility into your inventory through our Command Center platform.

VALIDATE
Receive ongoing managed services to support the invoice lifecycle, including contract management, expense validation, dispute resolution, and AP/GL feeds for payment.



From procurement and provisioning through inventory and expense management, we optimize your communications solutions across voice, data, cloud, and mobility. Advantage is your team behind the scenes—so you can focus on success.

Learn more at AdvantageCG.com

info@AdvantageCG.com | +1 212.872.1700

Advantage