Security Starts at the Edge:

The 2019 Security Buyer's Guide

Security is the foundation of digital business innovation.

It's a bold claim; one that hasn't always been accepted as truth. In the not so distant past, digital security was seen as a cost center. Those days are gone.

Security is essential to the success of any digital business. If there is one thing you can always count on, however, it's that security-related incursions are inevitable. And it's news to no one to say that these disruptions can have dire consequences beyond downtime. Security breaches erode trust and damage reputation.

Simply put, there's no longer a choice. As a CIO, CISO, or other security or IT leader, you know it's your job to be the central agent stressing the connections between business and digital risk. It's your responsibility to find the talent and technology to ensure the protection of your digital assets.

According to Gartner, by 2020, 100% of large enterprises will be asked to report on their cybersecurity and technology risks to their boards of directors at least annually. That's up from 40% in 2018. Whether you're a leader of a large enterprise or a smaller business, part of your ongoing security, risk management, and compliance strategy will be sourcing the most effective security solution for your business.

We know. Easier said than done. To help, we've compiled this guide for you to find the right solution for your business to scale resilience, build trust, and drive revenue.

Security leader, know thyself.

The ultimate question: What is the best solution to mitigate risk? To answer this question, you must first answer a few others: Who are we as a business? What are our requirements? What are the outcomes we're looking to see as a result of this purchase? Here's where to begin:

Assess your risk.

Good risk assessment rigorously evaluates an organization's current security posture. It begins by identifying potential threats to the organization and rating each threat based on its likelihood of occurrence as well as the potential impact if it occurs.

After flagging potential threats, the next step is to identify your vulnerabilities, such as a web server running an unpatched operating system with known security flaws or insufficient network bandwidth to absorb a DDoS attack. Also, as businesses migrate applications to the cloud, it has changed the way employees access them. No longer is it viable to provide unfettered access based on an outdated security model built around the false idea of an impenetrable perimeter.

Now you're beginning to focus your efforts on areas where threats and vulnerabilities overlap. Next comes a gap analysis. What controls do we need, that we don't already have, to mitigate these threats?

Security should not hinder business. It should instead be a business enabler.

Reminder: User experience and security do not need to be at odds.

Security should not hinder business. It should instead be a business enabler. These days, there is simply no tolerance for poor user experience. Whether your job is to protect an online retailer or the OTT delivery of an organization, end users expect perfection, with no downtime and no delay.

But often, while securing the network, user experiences are affected in adverse ways. The old adage says that on a fundamental level, user experience and security are at odds. It doesn't have to be that way.

Security solutions that introduce glitches to the user experience are just one example. Other pitfalls include security that unnecessarily disrupts applications or hamstrings developers. Some security providers even prevent internal teams from deploying their applications in the cloud provider of their choice. Again, it doesn't have to be this way.

Your next security vendor should satisfy these 4 critical elements.

After answering the questions above and getting a thorough sense of your objectives, it's time to turn your attention toward potential vendors. As you do so, first focus on the following critical elements that any quality security platform should deliver:

The Platform: The value of a security platform depends on you and your business needs. Ask yourself these questions when determining the critical elements a platform should provide for you: What does security platform mean to you as a security leader? What capabilities is it offering you? Is it enabling you to move faster? How is it securing your assets? How easy (or difficult) is it to manage?

Service and Support: Your next vendor should leverage highly trained security experts who provide threat analysis and personalized strategy. For many organizations, protecting against wide-ranging and constantly evolving security threats requires more than just technology. Faced with competing business objectives and a limited IT budget, you may not have the time, resources, or expert staff necessary to provide the best possible security for your sites, apps, and APIs. Managed security services could help decrease response time while increasing mitigation quality by leveraging a collective approach between you and the vendor.

Compliance: Make sure any vendor you're considering has all the appropriate compliance regulations covered for your industry, including EU General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), Federal Risk and Authorization Management Program (FedRAMP), ISO 27002, Service Organization Control (SOC) 2 Type II, and others.

Lastly, does the solution check all the boxes?: There are certain functions any security vendor must master and address to your satisfaction. The following are the basic must-haves you should keep top of mind as you dive into your vendor selection process.

- ❑ DDoS Mitigation
- ❑ Application Security
- ❑ API Security
- ❑ Phishing Prevention
- ❑ Credential Stuffing Protection
- ❑ Bot Detection
- ❑ Secure App Access
- ❑ Malware Protection

A security solution should protect your people and apps, and defend against bots and fraud.

What are the overarching benefits every solution should provide?

A security solution should provide your organization with three overarching benefits: **scale, visibility, and intelligence** – all while protecting your people and apps, and defending against bots and fraud. A new solution should help you move to a Zero Trust model to protect your people, shield revenue and customer experiences from bots and fraud, and perhaps most importantly, protect apps and APIs – the cornerstones of the modern digital experience.

Scale: As attacks grow in both size and speed, it is critical that any solution you are considering is able to keep up with evolving threats. In 2018, a 1.3 Tbps DDoS attack, driven by memcached reflection, threatened to unleash havoc. The record-breaking attack was more than twice the size of the notable Mirai botnet attack in 2017.

We are living in a world where malicious bot traffic will continue to hit unprecedented heights. Today's hackers use bots to launch pre-attack scans, exploit vulnerabilities, and execute a variety of attacks – code injection, DDoS, and password-guessing hacks – against your web-facing properties. These bots also commit fraud by credential stuffing, repetitively making and canceling purchases, holding and/

or consuming inventory, scraping sites, stealing information, and a host of other unwanted activities. In the worst of cases, a malicious bot can cause application and API outages, resulting in revenue loss.

The best method of removing the vast amounts of unwanted traffic is to eliminate the traffic at the *Edge*, before it ever reaches your websites. Complicating the issue, however, is the fact that legitimate bot traffic is a necessary part of the Internet. Having malicious bot protection and the ability to manage legitimate bot traffic is a critical attribute for any solution you consider.

There is also the issue of **scale for managing corporate apps.** And maintaining and supporting highly distributed applications is made even more difficult with rising user expectations. Apps are everywhere all the time. They are highly distributed among a far afield workforce — in some cases, across the globe.

What's more, apps are increasingly architected and assembled from disparate sources — frameworks, scripts, various content sources, and real-time code execution that happens from a multitude of places. You need a solution that can scale to match that distribution.

Visibility: If you don't have visibility into attacks, you can't derive actionable insight about how to better protect your customers in real time and mitigate the threats in the future. The strongest of security platforms interact with billions of devices and hundreds of millions of IP addresses every day, and see billions of DDoS attacks every year. The solution you choose needs to have this kind of reach to bring you visibility into the existing threat landscape.

A common refrain about serious breaches is "the hackers were able to work undetected for X months." And "once the bad guys were in, they were able to move around the network unhindered." Look for a solution that can provide a combination of more granular app access logging and control, with DNS-based threat protection. This will give you more visibility and reduce time to breach detection.

Also, a security solution should provide visibility after an attack in addition to providing real-time support. A security operations center should offer a real-time, single point of contact for attack support and real-time incident response against a wide range of threats. Then, after an attack, it should help you go beyond high-level dashboards and gain granular visibility for post-attack forensics and root-cause analysis.

You may want to investigate whether or not a potential platform allows you to manage multiple solutions through a single, unified portal for visibility into attacks and policy control. It should also have the ability to integrate with your existing SIEM (security information and event management) tool for greater awareness and visibility across all your security solutions.

Intelligence: Along with network capacity, your next solution needs to provide expertise that the ever-growing threat of volumetric DDoS attacks demand. A standout solution should be able to provide zero-second DDoS mitigation through a security operations center, staffed with industry experts that provide always-on monitoring, scrubbing, and DDoS mitigation services.

Protecting your apps, APIs, and users is about more than just capacity — it requires threat intelligence. Artificial intelligence and machine learning play a major part in delivering intelligence you can use to improve your security posture. Seek out platforms with far-reaching Internet visibility, great scale, and global distribution, combined with cutting-edge data science capabilities.

A vendor that can check these boxes should be able to offer adaptive threat and access protection, and in-depth threat intelligence, by leveraging well-fed machine learning engines. A combination of humans and algorithms should perform statistical, trend, and pattern analysis of structured and unstructured data to identify and mitigate new attack vectors before anybody else.

When you deploy security at the Edge, you are protecting your assets closer to the attack itself and moving digital experiences closer to users.

8 things your security solution must do for your organization.

So far, we've provided a framework for starting your security platform selection process and critical areas to focus on as you continue your research. Now let's get down to brass tacks. What are the key things your next security solution must do for you?

Keep your business running: Performance is critical, but availability is essential. Downtime and outages have a detrimental effect on revenue, productivity, and reputation — the very existence of your business. Security is simply non-negotiable for digital business and innovation. Your next security solution should enable quick and accurate mitigation. It should be able to identify and knock down threats. Period.

Secure your apps and APIs: APIs are the building blocks of modern applications and the connective tissue between companies that power modern, seamless user experiences. Organizations need hundreds of APIs, extending the attack surface beyond traditional bounds. Each API is a potential point of failure in terms of security, stability, and scalability. The answer is a cloud-based web application firewall (WAF) that provides a layer of security between the cloud deployments and consumers that want to access the data, protecting websites and APIs against opportunistic and persistent targeted attacks.

Achieve a Zero Trust environment: You need a security platform that provides a framework that only delivers apps and data to authenticated and authorized users, allows inline inspection and logging of traffic, prevents malware and DNS-based breaches, protects end users from phishing attacks, can identify and block bot traffic, connects to modern SaaS applications as well as legacy data center apps, seamlessly integrates with a WAF to mitigate application layer attacks, and provides clientless application access while ensuring those applications are fast and reliable. In short, you need a platform that fits your unique enterprise and enforces only allowed interactions between your data and your users.

Provide security at the Edge: When you deploy security at the Edge, you are protecting your assets closer to the attack itself and moving digital experiences closer to users. In essence, you're deploying a single pane of glass, an extension of your infrastructure, that sits between you — your users, your digital experiences — and the always-changing nature of today's digital environment. In a sense, it's a question of physical topology. At a time when users expect seamless digital experiences on demand, pushing interactions to the Edge — closer to the source of the data being generated — not only provides better experiences, but it is also the best location to construct safeguards between your business and your widely distributed users and consumers of digital experiences.

Outsmart advanced threats: Some threats are specifically designed to outmaneuver security tools. Your new security platform must be able to be one step ahead and outsmart these advanced threats. It's critical that any security vendor underpin their technology with security experts who research at the bleeding edge of malicious actors' methods. Security solutions must leverage technology and human expertise to keep up with or even anticipate the next zero-day attack.

Streamline your security controls: Your next security solution should empower you to become more agile by leveraging automation and scripting (orchestration). Our premise is that digital security is the foundation of business innovation — and therefore, growth. You want a solution that allows you to derive value faster by helping you become more efficient during your digital transformation.

Provide support 24/7: It may not be enough for your organization to rely exclusively on automated anti-DDoS tools or bandwidth reserves for DDoS detection and protection. It's likely that you'll benefit from having access to expert mitigation staff 24/7/365. An always-on security operations center with a global presence to respond to attacks whenever and wherever they happen, along with globally distributed scrubbing centers, ensures a more robust security position capable of deflecting even the largest and most sophisticated attacks. The combination of people and technology can make the difference between mediocrity and excellence. Decide whether or not your business requires managed services.

Protect your brand and instill customer trust: Essentially, trust is the lifeblood of your business. And it's what's at stake when it's your job to protect your business and mitigate risk.

Security leaders must help to equip their digital business with the mindset, resources, and planning to recover from inevitable disruptions. Failures anywhere in the ecosystem can have a cascading and detrimental effect on the business. With security no longer simply a cost center, you have the opportunity to enable digital transformation, drive revenue, and solidify yourself and your team as the foundation of the business and innovation.