softchoice

Softchoice

& Cross-Category Security

● ○ ○ ○ ○ ○ ○ ○

Overview

In October 2019, the Softchoice team hosted a panel discussion to explore the biggest issues in security today and how to address them. Chris Pratapas, Director of Business Development for Security at Softchoice joined four Softchoice technical solution architects to examine a variety of pressing issues.

These include continued shortage of experienced cybersecurity personnel and the complexity involved in protecting a company's data and applications in the cloud.

Adapting to today's security issues means moving beyond the traditional siloed approach to security. IT treated vulnerabilities affecting a particular system or cloud service in isolation. Instead, organizations should consider investing in cross-category security, which spans both on-premises and cloud-based infrastructures. But doing so requires not only developing the ability to produce real-time insights, but also access to a broad partner ecosystem.

In this guide, we'll review the key highlights of their discussion, along with steps your organization should be taking to modernize its overall security posture.

Issue #1

Navigating the Cybersecurity Skills Shortage

In the past decade, the number of relevant security threats and the amount of personnel available to handle them trended in opposite directions:

- Ransomware attacks were almost nonexistent in the early 2010s but surged to several hundred million incidents per year from 2016 to 2018.[1]
- The general proliferation of threats also meant that many organizations were attacked multiple times. In fact, FireEye found that 64% of companies attacked in 2018 had been retargeted, up from 56% the previous year.[2]
- Meanwhile, almost 3 million critical cybersecurity jobs are still unfilled worldwide, according to (ISC)2.[3]

Short-handed security teams struggle to keep up with the volume and velocity of cyberattacks coming their way. To keep up, they rely on a mix of manual processes. But these are both siloed and time-consuming. Work gets duplicated or performed in vain, producing false positives, all while threats proliferate.

[1] www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/

[2] content.fireeye.com/m-trends/rpt-m-trends-2019

[3] www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&amp;hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0\h

Issue #2

Simplifying the Overwhelming Complexity of Modern Cybersecurity

There's a now-famous chart entitled "CYBERscape: The Cybersecurity Landscape" that attempts to present all of the important vendors in the security sector. With so many names in each of the segments for "network security," "cloud security," and so on, it's quite difficult to read.

Nonetheless, the CYBERscape overview presents an accurate picture of the overwhelming volume of security-related information organizations need to track. From securing data centers and workloads in the cloud to ensuring all applications are patched and up-to-date,

Say, for example, your business was in the midst of setting up new workloads in Microsoft Azure. Threading the security needle here would require complete knowledge of the native capabilities available in that cloud, along with gaps to be filled and the vendors capable of filling them.

An end-to-end partnership, with a managed services provider well connected to Microsoft and other security firms, can simplify the decision-making process. Rather than trying to determine which of the thousands of possible vendors would be best, you can rely on expert recommendations.

An end-to-end partnership, with a managed services provider well connected to Microsoft and other security firms, can simplify the decision-making process.

○ ○ ○ ● ○ ○ ○ ○

Issue #3

Taking Responsibility for Cloud Security

Moving IT infrastructure, development platforms and business software into the cloud has some decisive advantages over hosting those same assets on-prem. At the same time, it creates new complications and liabilities, as illustrated by a string of incidents in 2019 involving the exposure of records on public cloud servers.

Misconfigurations are a common cause of such breaches. They also point to a larger issue: clarity around where security and risk management responsibilities fall between the organization and the cloud service provider.

For instance, in **software-as-a-service (SaaS)** the CSP secures the host, middleware and application, whereas in **infrastructure-as-a-service (IaaS)** the customer maintains responsibility for these components.

When IT teams are understaffed and overwhelmed, though, the burden is often too much to handle. Almost two-thirds of publicly disclosed incidents on public clouds are the result of the misconfigurations mentioned above.

To mitigate the risk of breaches in the cloud, it's imperative to think about workload protection at the earliest stages of the cloud journey.

Moreover, working with experienced security partners, capable of incorporating the right controls for each type of infrastructure into a coherent enterprise-wide framework, much improves chances of success.

Cross-Category Security

The Path to Modernized Cybersecurity

Overcoming operational complexity and the shortage of cybersecurity experts requires taking a fresh approach that replaces siloed and manual workflows with a unified strategy supported by more automated technologies.

Identifying potential vulnerabilities in any environment is essential, as is finding the corresponding controls and vendors to help remove them.

This is where Softchoice can assist in the creation of a cross-category security reference architecture, which accounts for all IT infrastructures in use and connects customers to a broad partner ecosystem that can fill any gaps therein.

Cross-category security can address public cloud environments like AWS, Azure and Google Cloud, providing insights into the built-in controls on each.

Their equivalent services on the other platforms (and in on-prem setups) and where third-party solutions may be merited to ensure full protection:

- In an on-prem setup, for instance, a SIEM is a pivotal cybersecurity component. On AWS, Cloudtrail supplies similar functionality.n Azure there are Monitor Log Analytics. So in all three cases, customers have immediate access to SIEM-like functionality.
- In contrast, standing up equivalent IPS/IDS protections in either AWS or Azure requires a third-party service, and the same holds for features like web filtering. Without cross-category security, this key gap between on-prem and cloud might go unrecognized.

○ ○ ○ ○ ○ ● ○ ○

Cross-Category Security

The Path to Modernized Cybersecurity

Overall, cross-category security provides several key benefits in the context of today's biggest cybersecurity challenges by:

1. Reducing duplicated effort that arises when teams work on projects in parallel and without knowledge of how a given set of controls fits into the larger security architecture.

2. Making it easier to combat multiple threats at once by outfitting each environment with appropriate and optimal protections, ranging from firewalls to anti-malware defenses.

3. Eliminating gaps that may have gone unnoticed due to an assumption that a particular control was built-in, when it in fact requires additional effort to implement.

An experienced IT solution and managed services provider can guide you on the road to cross-category security, helping with everything from an initial gap assessment and assistance with penetration testing, to the selection of specific vendors with effective, up-to-date solutions for the environment in question.

○ ○ ○ ○ ○ ○ ● ○

Selecting the Right Vendors

The Softchoice Approach to the Partner Ecosystem

Speaking of vendors, remember the CYBERscape chart we talked about earlier? It would seem like an insurmountable obstacle to cybersecurity modernization, since organizations lack the bandwidth to vet every single possible option for suitability in their environments.

The good news is that customers don't have to perform this level of due diligence on their own. Instead, they can tap into a vast partner ecosystem that has been carefully categorized by specialty and screened for quality by a managed services provider. This is how the Softchoice Security Line Card works.

Softchoice identifies key partners in every major area of security, with 52 vendors across 38 categories. When a customer needs a specific solution to shore up their cloud environment, our team can recommend an appropriate partner.

Our strategic partnerships also continue to evolve alongside changes in the cybersecurity landscape as a whole. That way, customers always have a relevant selection at their fingertips to guard against new and emerging threats, from ransomware to exposed vulnerabilities in public clouds.

Conclusion

As the 2020s begin, cybersecurity has never been a more strategic concern for companies of all sizes. Simply put, protecting critical data and IT infrastructure is integral to organizational survival.

There are strong headwinds facing IT security teams,—including but not limited to a shortage of security personnel, a complex set of responsibilities and difficulty managing multiple cloud services. But taking a holistic approach such as cross-category security provides a sustainable way forward.

This guide scratches the surface of our panel discussion on cybersecurity.

To take a deeper dive watch the full session.

Ready to learn more about our security solutions and partners? **Get in touch** with Softchoice.

About Softchoice:

Softchoice is one of the largest IT solution and managed service providers in North America. Every day, thousands of organizations rely on Softchoice to provide insight and expertise that speeds the adoption of technology, while managing cost and risk.

Through our unique points of view, we challenge leaders to think differently about the impact of technology on their employees and customers.

Softchoice enables organizations to realize the full benefits of public cloud and a modern IT infrastructure through solution design, implementation, asset management, and assessment services, as well as ongoing support and mentorship through managed services.

With access to one of the most efficient and cost-effective technology supply chains in North America, Softchoice also ensures products get to our customers quickly and in a trouble-free way.