BUYER'S GUIDE TO

CYBER SECURITY

Sponsored by Cyber Talk

Detection and Defense Now Present More Challenges Than Ever Before

For organizations worldwide, intruders executing Advanced Persistent Threats (APTs) and sophisticated attacks are growing increasingly common. These activities pose an extreme danger, potentially resulting in data loss and/or infrastructure damage that can precipitate an organization's demise.

APTs and other sophisticated threats can lurk in a system for days, weeks, months or even years at a time, quietly gathering data. Such compromises are extremely problematic, as they take a long time to pick up on.

The calculus required for success in these endeavors means that they're mainly executed by sizeable, often state-backed, hacker groups, and that the attacks are more sophisticated and elusive than standard malware or ransomware attacks.

In addition to the proliferation of APTs, the multi-vector attacks and polymorphic nature of modern cyber attacks also differentiates them from those of years past.

A QUICK HISTORY LESSON

- **Cyber threats first developed in the 1980s, with the mass availability of personal computers.**
- **These were followed by attacks in the 1990's that precipitated the development of the network firewall.**
- **In the early 2000s, we saw attackers leveraging a wider array of vulnerabilities, and by the early 2010s hackers had developed sophisticated maneuvers, such as APTs.**

Securing Vulnerable Organizations Against Advanced and Sophisticated Threats

In recent years, advanced and sophisticated attacks have occurred across sectors, from manufacturing to telecommunications to healthcare to the financial sector to the public sector.

Some of these sectors, like the public sector, are required to keep operating daily, meaning that they must continually play defense against cyber attackers. However, other sectors include private enterprises that may have to shutter their doors after experiencing a cyber attack. For these types of enterprises (often SMBs), there's no government funding, and there are no bailouts. Rather, strong threat prevention is uniquely imperative.

As organizations of all kinds deploy IoT (Internet of things) technologies, and stay connected via smartphones, the dangers only multiply. These days, an attack that begins within a smartphone can go through an organization's cloud, and can end up shutting down the data center. The cloud, autonomous cars, and millions of connected IoT devices require a scalable and well-rounded approach to security.

Security experts advise organizations, especially the most vulnerable ones, to think about cyber breaches not in terms of 'if', but in terms of 'when'.

To that effect, understanding the core elements required for top-tier cyber security is a must. Applying innovative digital defense is mission-critical for the survival of any modern organization. Dig into the Cyber Talk Buyer's Guide to scope out key considerations when it comes to improving your cyber security architecture.

This buyer's guide provides in-depth strategies that can help you realize new goals and that can assist in enhancing your organization's security posture.

DID YOU KNOW?

- **More than 90% of organizations are using outdated cyber security tools.**[1]
- **77% of security professionals anticipate a significant breach in the near future.**[2]
- **By 2021, cyber damages will total more than $6 trillion, worldwide.**[3]
- **Through 2022, 95% of breaches will likely occur as a result of customer misconfigurations, or other human errors.**
- **42% of storage objects evaluated with recorded data loss prevention incidents were misconfigured.**[4]

[1] InfoSec Newsflash, Cyber Security Statistics for 2019, Cyber Defense Magazine, March 21, 2019
https://www.cyberdefensemagazine.com/cyber-security-statistics-for-2019

[2] Jaikumar Vijayan, 31 cybersecurity stats that matter, TechBeacon, September 30, 2019
https://techbeacon.com/security/31-cybersecurity-stats-matter

[3] Matt Powell, 11 Eye Opening Cyber Security Statistics for 2019, CPO Magazine, June 25, 2019
https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019

[4] Charlie Osborne for Zero Day, 99 percent of all misconfigurations in the public cloud go unreported, ZD Net, September 24, 2019
https://www.zdnet.com/article/99-percent-of-all-misconfiguration-in-the-public-cloud-go-unreported

10 Most Important Considerations in Choosing Your Cyber Security

1. REAL-TIME PREVENTION
2. IDENTIFICATION
3. INSPECTION WITHIN SSL/TLS
4. GOING BEYOND SIGNATURE-BASED DEFENSES
5. PROTECTION FROM EVERY DIRECTION
6. A ZERO TRUST APPROACH
7. SHARED THREAT INTELLIGENCE
8. CONTROL THE CLOUD
9. UNIFIED MANAGEMENT CONFIGURATION
10. SECURITY FROM THE START

Read on for an in-depth discussion of each component.
To get started, we'll take a look at a few key concepts.

UNIFIED AND EFFICIENT SECURITY

Having unified management control across all networks, clouds, mobile, and endpoint environments increases operational efficiency and reduces complexity. Unified security can cut operations time by as much as 80%. It scales easily, and also offers the highest caliber of prevention. Unified management is an important feature as you build your next-generation security architecture.

SHARED INTELLIGENCE

Threat intelligence is known as one of the most proactive and effective security solutions available. Threat intelligence products that gather information from expert feeds, enriched by research from expansive security research teams, enable automated remediation processes, reducing manual operations for your team. The reliable real-time data can also help you make the right decisions in the face of threats. In this buyer's guide, learn why embedded threat intelligence is an important feature of your security architecture.

NETWORK

When thinking about network security, you'll want to know which applications your users are running within your network, and then you'll want comprehensive visibility, combined with flexible enforcement points around applications. Gaining insights into and taking control of what your users are doing can help you secure your network.

MOBILE

Nearly every enterprise allows employees to bring their mobile devices (BYOD) and to use them in conjunction with company resources. As a result, organizations deploy safeguards that protect business data, provide secure mobile access to business documents, and that keep mobile devices safe from threats. Obtaining security that can protect a wide range of mobile devices is essential.

> By keeping all of these concepts in mind, you'll develop a robust security architecture to defend against today's threats, and tomorrow's.

CLOUD

The cloud has become an integral piece of architecture within many organizations. When it comes to cloud security, the shared responsibility model means that the onus falls on the administrator to secure the data, not the public cloud vendors (contrary to some perceptions). This can present a major challenge for organizations, and some try to skimp on cloud security measures. However, robust cloud security can assist in reducing costs, and enhancing reliability. This guide can show you the additional advantages of investing in more comprehensive cloud security.

ENDPOINT

You'll want endpoint security that can be managed centrally using a single management console, as this allows for simple and flexible administration, and increased security. In addition, non-traditional endpoints mean that you need security that can keep up. The buyer's guide can help you identify the right endpoint security for your organization.

1 Prevent in Real-Time

A cyber attack can shake the foundations of an organization, negatively impacting the entire business. Avoid attacks before they can take root. Get security that's designed to prevent, not just to detect.

Your prevention platform should include cutting-edge technologies, like behavioral detection and machine learning algorithms that can identify and block exploits on networks, cloud, and endpoint, before they execute and infiltrate your network. The ability to prevent patient-zero, so to speak, is critical. Get a real-time prevention platform with rapid responses to new vulnerabilities and a high malware catch-rate. As a starting point for developing a shortlist of vendors to work with, look for vendors with NSS Labs recommendations.

The payoffs of investing in prevention are profound. Applying cyber security prevention can streamline protections across your system (networks, cloud, endpoint, mobile, and IoT), improve efficiency and reduce your costs. All of these advantages can help you add value to your organization.

2 Identifying Users, Applications, and Devices From All Sources

You need a solution that gives you full visibility into who's on your system, what they're doing and where they're going, no matter whether the activity is on your networks, cloud, mobile, endpoints, or IoT devices.

Receive accurate, real-time information about who's browsing through your resources. An IP address isn't good enough. Find out the precise identity of each user who's accessing your organization's assets.

Obtain up-to-the-minute information about what's on your system. Your mission-critical applications (and data) are perpetually at risk. An alarming **37%** of security risks occur within the application layer, with SQL injections (SQLI) and cross-site scripting (XSS), comprising more than 15% of these events.[5] The race to build and deploy quickly can mean that application layer vulnerabilities go unnoticed. And within the applications and data sets, where is the information going?

Get a security solution that offers comprehensive visibility and granular insights so that you can act quickly, and protect your critical infrastructure.

[5] Hamsa Srinivasan, What's the Best Strategy to Manage Application Security Risk, Security Intelligence, July 6, 2018 https://securityintelligence.com/whats-the-best-strategy-to-manage-application-security-risk

3 Uncover Attacks Hiding Within Encrypted Traffic (Inspect Within SSL/TLS)

Organizations that apply SSL/TLS, ensure that a third-party cannot sit between the server and the browser to read or manipulate electronically transmitted information. Any bad actors will only see a garbled mess of alphanumeric text.

Research indicates that only **3.5%** of organizations decrypt their network traffic in order to fully inspect it.[6] Reluctance to inspect often comes from concerns about reduced firewall performance, loss of privacy, and creating a sub-par end-user experience, **among other factors**.[7] In addition, if SSL/TLS interception is executed poorly, the initiative can do more **harm** than good.[8] However, when executed well, SSL/TLS inspection can significantly improve security.

From 2016 through the present, the percentage of websites protected with the SSL/TLS protocol, as executed through HTTPS, has increased from 40% **to over 80%**.[9] HTTPS can protect users against man-in-the-middle (MitM) attacks, malicious content, and more. It stops credit card and identity theft. Without it, you're blind to a large portion of your company's traffic.

Google now uses HTTPS as a search ranking signal. This means that investing in SSL/TLS will not only improve your security, it will also improve **your organization's SEO**, making you more competitive within your marketspace.[10] These days, browser makers are doing all but demanding that websites apply HTTPS before displaying pages to web-users, and pressure from the general public is also mounting.

A lock icon on your site may be tiny, but the protection that it affords and trust that it generates could be huge.

4 Threats Can Get Past Signature-Based Defenses: Here's What to Do

Signature-based defenses have been an organizational go-to since the early 2000s.

However, the strength of a security system can no longer be measured by the number of malware signatures included in a vendors' library of threats. Anti-virus and intrusion prevention products are only updated with "known" attacks, and fail to protect organizations from threats that exploit signature-based defenses by new variants and/or zero day attacks.

[6,7] Zeljka Zorz, What is flowing through your enterprise network, Help Net Security, February 20, 2020
https://www.helpnetsecurity.com/2020/02/20/firewall-tls-inspection

[8] Lucian Constantin from IDG News Service, It's time to turn on HTTPS: The benefits are well worth the effort, Computer World, March 14, 2017
https://www.computerworld.com/article/3180690/its-time-to-turn-on-https-the-benefits-are-well-worth-the-effort.html

[9] Nicole Casal Moore, How Let's Encrypt doubled the internet's percentage of secure websites in four years, Michigan News, November 13, 2019
https://news.umich.edu/how-lets-encrypt-doubled-the-internets-percentage-of-secure-websites-in-four-years

[10] Lucian Constantin from IDG News Service, It's time to turn on HTTPS: The benefits are well worth the effort, Computer World, March 14, 2017
https://www.computerworld.com/article/3180690/its-time-to-turn-on-https-the-benefits-are-well-worth-the-effort.html

Organizations must step up to the plate with measures to protect themselves from unknown threats. Cyber security platforms that can protect all vectors, including cloud, mobile, network, and IoT, are your best bet. Invest in a platform that offers:

- Sandboxing (static, dynamic, and behavioral analysis)
- CDR (content disarm and reconstruction), hence, sanitizing documents
- Artificial intelligence/ machine learning
- Threat cloud

All of these components can help you stay ahead of the hackers.

5 Threats Can Come From All Directions: Protect Everywhere

Locking down everything is critical. The only way to ensure that your network is secure is by ensuring that everything connected to it is secure. Secure your individual computers, phones, tablets, and other extensions of your network.

An ever-growing number of hackers are capitalizing on these vulnerabilities because organizations often lack sophisticated tools to protect against advanced threats.

Whether your organizations' data is at rest, or in motion via the cloud or on mobile devices, be sure that you have proactive and continuous protection.

Comprehensive protection is critical. In its absence, points of failure can go unnoticed, leading to major breaches, like the high-profile **Equifax breach of 2017**.[11] In the case of Equifax, a vulnerability that should have been patched represented the first point of failure. Subsequent failure points included non-segmented networks, and an outdated encryption certificate. Higher caliber security architecture could have detected the breach more quickly.

For comprehensive protection, get a security platform that offers simple deployments, with minimal maintenance demands. The majority of Security Operation Center (SOC) teams have too many items to attend to as it is. By reducing the maintenance needs, your team can focus on the important aspects of security, maximizing the value of employee labor, and the value of the product.

[11] Amol Sarwate, Do You Know What's Hiding in Your Public Cloud, CloudPassage.com
https://www.cloudpassage.com/resources-cloud-security-compliance-whitepaper/?gclid=Cj0KCQiAhojzBRC3ARIsAGtNtHU4H9KxvFdVeo73mJXCVjW09IBCENODQImApU0jSF7ebKR7k4hIRw0aAuq-EALw_wcB

For example, with contemporary security platforms, you can block a malicious website on a user's phone, and then the architecture will automatically block it on the same user's desktop and laptop. This saves your team time, and demonstrates how new security products enhance your capabilities.

In protecting every vector, you'll also want a solution that can offer advanced threat prevention, forensics, and a remote access VPN solution.

DID YOU KNOW?

- **For a business, the average cost of cyber attack could be as much as $3.92 million.[12]**
- **In the past three years, organizations have contended with the loss of over 11.7 billion records.[13]**
- **For the most part, the lifecycle of a breach adds up to 279 days.[14]**

6 Guard Against Insider Threats With Zero Trust

Protecting the security perimeter from cyber threats used to be enough. Once a user, application or device was inside, it could be trusted. Now, the business environment has expanded and the perimeter is everywhere.

The key to overcoming the challenge of "perimeter everywhere" is a Zero Trust architecture. Zero Trust is the way to handle the increased propensity for connecting everything to the network. The surest bet is not to trust anything, and to move trust down to the user/device, forcing each user/device earn trust before syncing with the network.

With the principles of the Zero Trust security model, you can prevent malicious lateral movement with granular network segmentation, use context-aware authorization to protect against identity-thieves, protect all devices from threats, and **more**.[15]

You'll be able to know who's on your network, what's on your network, where it is coming from, where the user, device or application is authorized to go, and what the user, device or application intends to do. The ability to limit permissions, access, and to track users enables you to prevent attacks.

It's a challenge to retrofit older architectures with Zero Trust approaches. Build Zero Trust into your systems as you invest in new technologies.

[12, 13, 14] Jamie Davies, 206 days: IBM's estimate on how long it takes to find a security breach, Telecoms.com, July 23, 2019
https://telecoms.com/498656/206-days-ibms-estimate-on-how-long-it-takes-to-find-a-security-breach

[15] The Ultimate Guide to Zero Trust Security, Check Point Software
https://pages.checkpoint.com/the-ultimate-guide-to-zero-trust.html

7 Shared Intelligence Means Better Security With Less Work

To have the greatest quantity of threat intelligence at your disposal, purchase a solution with shared threat intelligence. Receiving intelligence from multiple streams, supplemented by research directly from incident response teams can help you see around blind spots. Shared threat intelligence enables you to see which threats are affecting your geographical locale, or your industry, specifically. When shopping for solutions with built-in threat intelligence, look for platforms that are:

- Accurate
- Aligned with your intelligence requirements
- Integrated
- Predictive
- Relevant
- Tailored
- Timely

Top-tier solutions can connect the dots for you, enabling you to quickly respond to threats, or to remediate where necessary. With comprehensive, shared threat intelligence, you can see the whole picture in full-focus, rather than a partial, blurry scene.

8 Control the Cloud

Organizations need the ability to easily manage security and compliance for cloud environments. The development of the public cloud allows organizations to scale, and to conduct business more efficiently, but the lack of borders also demands an entirely new level of security. As a result, we're seeing more cloud challenges than in the past. We'll describe why you should take control over your cloud security, and show you how to do so.

- Cloud hijacking is a growing concern. A variety of measures should be taken to protect against compromised credentials and identity theft, including the encryption of sensitive information before it's placed in the cloud, MFA and more. As an added layer of security, consider a solution with just-in-time privilege elevation with out-of-band authorization for IAM actions. Limit access, but also retain the capacity to modulate controls.
- In controlling your cloud, you'll also want to be able to easily visualize and assess your security posture, quickly detect misconfigurations, actively enforce best practices, and mitigate risk through simple remediation. With a consolidated cyber security solution, you can accomplish all of these things through a single management console, bringing agility to the security and compliance lifecycle.
- Hassle-free cloud compliance and governance are critical. Security teams are often beyond busy, and the magnitude of this endeavor frequently exceeds employees' capacities. Look for security with comprehensive compliance management, including automated, continuous compliance that can help assess and enforce best practices.

9 Managing a Unified Configuration

Synchronize your security. Centralized security management reduces complexity, strengthens security, improves workflow, and reduces human errors.

Buying one security management console that can offer forensics for cloud, mobile, networks, and endpoints dissolves the complexity that comes from managing different consoles, policies and logs.

When you invest in a single security management console, you not only reduce complexity and improve security, you also improve workflow. Multiple consoles means toggling back and forth across 10 or more different systems, leaving some systems unattended while you examine others. As a result, you and your team may see threats belatedly, giving them ample time to cause preventable system damage. A single management solution presents all of the insights upfront, cutting down on management time, and allowing you to rapidly triage any outstanding challenges.

Lastly, owning multiple solutions that are not interoperable requires security professionals to manually enter data into different platforms. Not only does this create the monotonous task of rekeying information, it also exposes organizations to data entry errors. With an integrated solution, data only needs to be entered once, cutting down on the risk of employee errors and strengthening your cyber security posture.

For any of a number of reasons, is not always possible for a given organization to adopt a fully consolidated approach. In this case, organizations can adopt a modular approach to security, gradually deploying individual security components over time in order to build a complete security posture. Depending on your budget, your labor force, or other constraints, this could be the best option for your organization.

10 The Security Vendor's Architecture Must Be Secure

Those who build security products are well versed in terms of how to build securely. Nonetheless, the occasional security vulnerability gets baked into an application. If this occurs, you'll want to be working with a company that reacts swiftly, and that can quickly provide patches (or alternatives) to customers.

In 2019, previously unknown vulnerabilities within a security vendor's system were exploited by a state-backed hacking group. Unfortunately, it took a long time for these vulnerabilities to be patched, and to this day, there are still customers running vulnerable versions of those solutions. This incident highlights the importance of choosing a vendor that has your back, and that's ready to take every action necessary to efficiently provide quality security.

Working with a mature, well-known security firm can mean the difference between consistent security, and rapid responses, vs. compromised systems.

Comparing the Competition

Decide on which vendor to work with by taking the ten key components of effective, advanced security and benchmarking them against actual vendors. To make things easy, we've taken the heavy lifting out of the equation for you, providing you with a brief analysis of who's who within the market space. Discover which vendors have security products that most closely align with the recommendations in this buyer's guide.

	KEY PLAYERS IN CYBER SECURITY MARKETSPACE			
10 Most Important Considerations in Choosing Your Cyber Security	Check Point SOFTWARE TECHNOLOGIES LTD	CISCO	paloalto NETWORKS	FORTINET
Real-Time Prevention	✓	✗	✗	✗
Identification	✓	✓	✓	✓
Inspection within SSL/TLS	✓	✓	✓	✓
Going Beyond Signature-Based Defenses	✓	✓	✓	✓
Protection from Every Direction	✓	Partial	Partial	Partial
Zero Trust Approach	✓	Complicated	✓	✓
Shared Threat Intelligence	✓	✓	✓	✓
Control the Cloud	✓	✗	✓	Partial
Unified Management Configuration	**7 Menus**	35 Menus for Same Tasks	32 Menus for Same Tasks	19 Menus for Same Tasks
Security from the Start	✓	✗	✗	✗

The analysis above can help you distinguish the signal from the noise.

Summary

In this guide, we've discussed each of the key components that you need to consider as you strive to improve your cyber security. Choosing the right security product depends on understanding the technological functions that will protect your organization from the latest threats. Now that you know what's on the market and which tools can provide unyielding and robust digital defense, you can make the best cyber security decisions possible for your organization.

Download a test plan for a next generation firewall. For additional cyber security resources, visit **Cyber Talk**.