SUMMER/FALL 2023

PALO ALTO NETWORKS

CYBER PERSPECTIVES

Security Consolidation

WHAT IT IS AND WHY YOU SHOULD CARE

CYBER LEADERSHIP

10 Cloud Security Risks Organizations Should Address

LATEST RESEARCH

2023 Unit 42 Attack Surface Threat Report Executive Summary paloalto NETWORKS | IGNITE ON TOUR

SECURING THE WAY FORWARD

Disruptive technologies, such as AI/ML, cloud computing, and IoT, have changed the game for cybersecurity. Today's cyber leaders need to make tough decisions and bold moves.

Join us for **Ignite on Tour**, an exclusive one-day cybersecurity strategy and networking event specifically for cybersecurity leaders and influencers.

We've refocused our traditional Ignite user conference, previously geared toward practitioners, to help cybersecurity decision-makers and influencers accelerate cyber transformation in the face of a rapidly changing threat landscape.

Our North America tour kicks off in October with stops in Dallas and New York City.

IGNITE ON TOUR DALLAS
October 19, 2023

IGNITE ON TOUR NEW YORK
October 25, 2023

CYBER LEADERSHIP

SECURITY AS A BUSINESS ENABLER

ARTIFICIAL INTELLIGENCE

HEALTHCARE

LATEST RESEARCH

CISO's Survival Kit for the Next Board Meeting

Dear Reader,

This Summer/Fall 2023 edition of the *Cyber Perspectives Magazine* marks the one-year anniversary since our first publication. To commemorate, we have included a special feature below compiling our go-to articles with the best advice for cybersecurity leaders. Additionally, this issue features an executive summary of our latest Attack Surface Threat Report, which leverages threat analysis data from our Cortex Xpanse and Unit 42 teams.

Since its first publication, the *Cyber Perspectives Magazine* has been a trusted resource providing valuable guidance and support to chief information security officers (CISOs). In today's digital age, the role of a CISO is more critical than ever. With cyberthreats becoming increasingly sophisticated and pervasive, it is essential for CISOs to not only stay ahead of the bad actors but also maintain the confidence of your organization's board. Many of you are being asked about artificial intelligence (AI). Check out the article on page 22, "ChatGPT: AI for Good or AI for Bad Camp."

We hope you find this issue useful. Please send us your comments, feedback, and content ideas to **magazine editor@paloaltonetworks.com**.

CISO Board Meeting Survival Kit

Below we have linked to our favorite *Cyber Perspectives* articles to create a CISO Board Meeting Survival Kit. These articles were specifically chosen to help prepare you for your upcoming board meeting. Whether you are new to the magazine or a regular reader, this guide will provide you with invaluable insights and strategies to confidently communicate your organization's cybersecurity posture, address potential risks, and present key initiatives to the board.

With this survival guide in hand, you can approach your next board meeting with confidence, ensuring that you effectively convey the importance of cybersecurity and drive informed decision-making to safeguard your company's digital assets. Scan the QR Code below to read these essential articles:

- "How to Explain Cybersecurity Transformation to Your Board"
- "Enabling Business and Security Together"
- "Attack Surface Risks, Challenges and Changes"
- "How to Answer Your Board's Questions on Cyber Risk Mitigation"
- "How to Answer Your Board's Top Cybersecurity Questions—Regulatory Compliance Requirements"

10 Cloud Security Risks Organizations Should Address

By Nathaniel Quist

Through advances in cloud technology, data access is now readily available. This is a boon for developers. For security practitioners, though, it presents a challenge. With datasets increasingly made available to company employees via cloud adoption or migration, the potential for personal and identifiable data falling into the wrong hands increases.

Implementing a robust and systematic security program to secure your cloud environment is the first step to ensuring sensitive internal data doesn't fall into those hands.

In this post, we will detail the top 10 cloud security risks every organization should address to prevent becoming the next cloud breach headline.

Top 10 Cloud Security Risks

In the recently released Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface,[1] Unit 42 and Prisma Cloud researchers identify 10 critical risks that require an architectural and operational focus to ensure the detection of advanced threats within cloud environments.

This list will assist organizational leaders across any industry and vertical to secure their cloud environments against cloud threat actors.

Tactical Goals for Top Cloud Threats

1. Failure to Properly Manage IAM Policies

Unit 42 researchers have curated an index of known cloud threat actors groups (CTAG)[2] that actively target cloud environments. You can view indicators of compromise (IOC) for each CTAG[3] under respective tags that include Automated Libra, Adept Libra, Thief Libra, Money Libra, Aged Libra and Returned Libra.

The link between these threat actor groups is their common IAM credentials target and use of automation to exfiltrate identifiable IAM credentials within seconds of compromising a cloud environment.

According to Unit 42's latest Cloud Threat Report, 83% of organizations have hard-coded IAM credentials within their source control management systems, and 76% of organizations don't enforce MFA for their cloud accounts.

Proper IAM policy creation is an essential security requirement for maintaining a secure cloud. To ensure your organization is adequately protected from IAM credential theft, consider implementing the following security measures:

- **Define a robust least privilege architecture** for each IAM role or policy, such as single-use isolated service accounts for all cloud developments.
- **Automate IAM credential cycling** to avoid long-lived credentials, defaulting to zero access for IAM user credentials when they elapse.
- **Alert on any modification or deletion** of any established IAM role or policy.
- **Alert on the creation of new** IAM users, roles, or policies.
- **Scan all modified cloud infrastructure as code (IaC) for leaked IAM data** and implement a remediation plan for positive findings. Pay close attention to access ID, keys. tokens, PII, and sensitive internal data.

2. Lack of Operationalization of Cloud Audit and Log Data

Cloud platforms, their services, and cloud-native applications generate vast quantities of data. This data is a gold mine for security operations and incident response teams if they can

»

access and view it. But 76% of organizations don't implement cloud storage audit logging policies within their cloud environments, according to Cloud Threat Report, Volume 7.

Many reasons prompt organizations to forgo logging cloud audit and infrastructure usage.[4] Logs are often noisy and expensive to store, but not having them can cripple security teams trying to detect and remediate a security breach.

To effectively store and use logging data, Unit 42 recommends implementing the following action items:

- **Enable CSP tools and services designed to reduce log noise** and extract necessary information.
- **Consolidate cloud log monitoring** to a third-party security monitoring application, such as Prisma Cloud, to coalesce the data across hybrid and multicloud environments. This also allows for the identification of cloud incidents affecting more than a single cloud environment.
- **Rank and prioritize critical logging sources and their events.** Prioritizing IAM and runtime monitoring logs from cloud sources to ensure that security researchers have the data needed to detect malicious operations as they occur.

3. Extended Response Times to Cloud Alerting

Once logging access is available to security teams, they can begin actively monitoring and hunting for threats within their cloud environments. But logging is only a foundational component. Responding to alerts is equally important to the long-term success of security teams.

But the average alert dwell time is 145 hours (6 days), according to Cloud Threat Report, Vol 7. What's more, researchers found that 5% of critical alerts were generating 80% of total alerts, introducing avoidable noise and contributing to alert fatigue.[5]

Implement the following tactics to help your security teams identify and respond to critical alerts in a timely fashion.

- **Enable time requirements** for alerts based on their criticality.
- **Address critical alerts first**. One alert often relates to and informs subsequent alerts. If a critical alert is corrected, it will address all related alerts.
- **Fine-tune alerting policies** based on organizational needs and GRC requirements.
- **Follow the guidance** of the Prisma Cloud alert creation process when creating custom alerts.[6]

4. Failure to Assess the Cloud Threat Landscape

Sixty-three percent of production cloud codebases contain unpatched vulnerabilities rated critical or high severity level, as reported in Cloud Threat Report, Vol. 7. If that doesn't give you pause, consider that 11% of the exposed cloud web services contain critical or high severity vulnerabilities—and 71% of these are at least two years old.

These two findings demonstrate that organizations should spend more time scanning their cloud infrastructure for vulnerabilities and misconfigurations, especially given that many cloud-based attacks are successful due to misconfigurations within cloud environments.

The following five tactics can give organizations solid ground in knowing and securing their cloud threat exposure.

- **Perform a quarterly asset inventory** and security assessment of their cloud services and resources.
- **Perform vulnerability and misconfiguration scanning** on all cloud assets prior to their production deployment.
- **Identify exposed systems and services** using network scanners.
- **Perform ongoing penetration testing operations** on cloud production environments.
- **Expressly specify that only the latest versions and patches** of containerized applications will be deployed to production.

5. Unaware of Cloud Threat Actor Group Operations

Sun Tzu said, "Know your enemy and know yourself; in a hundred battles you will never be defeated."

When you know your cloud threat landscape, you're halfway there to defending it. And though it may seem like an onerous endeavor, you'll find numerous resources available to assist you, including Unit 42's Actionable Threat Objects and Mitigations (ATOM).[7]

The following tactics can help your organization to identify CTAGs important to your operations and what actions they can take to mitigate these actor groups.

- **Subscribe to several threat intelligence platforms**, such as Unit 42's Taxii feed,[8] that offer STIX/TAXII IOC data consumable by your organization's security tools.
- **Identify which CTAGs** target your industry's vertical.
- **Develop detection solutions and alerting policies** for identified CTAG operations.
- **Implement prevention mitigations** that will outright block specific IOCs.
- **Train security staff on cloud attack techniques** and operations to be better equipped to identify breaches.

6. Failure to Detect and Properly Handle Cloud-Targeting Malware

Cloud endpoint runtime monitoring is available for many organizations using single and multicloud platforms. Runtime monitoring for virtual machine, container, and serverless cloud instances are required of organizations that want to know if their cloud instances operations were designed to perform (i.e., interacting with known command and control (C2) nodes or running malicious binaries post-compromise). »

With 63% of production cloud codebases containing a vulnerability of high or critical severity level, the need to monitor cloud instances is greater than ever. Tactical measures an organization should take to ensure they can view runtime operations within their cloud instances include:

- **Deploy and properly configure cloud workload protection** (CWP) to VM, Cluster and Container hosts, and serverless functions
- **Ensure CWP solutions are configured to query backend** Threat Intelligence data stores such as Wildfire
- **Implement alerting, prevention, and secure** handling policies for identified malware

7. Redundant Security Tool Operations

Several security tools available to detect security threats might seem logical. After all, redundancy is a key component to ensure visibility. But for 76% of organizations, the use of multiple point tools creates blind spots.[9] With more security tools in place, more time is required to configure those tools, and once tools are established, the number of alerts climbs, exacerbating alert fatigue among security professionals.

In light of these facts, Palo Alto Networks researchers recommend the following tactics:

- **Reduce the number of independent or redundant security tools** allowing the organization to streamline its security operation effectiveness.
- **Integrate security tools** that provide a unified platform to ensure reduced gap coverage.[10]

8. Multiple Cloud Operation Owners

In a recent Unit 42 IR case, researchers were tracking the actions of a CTAG that gained access to an organization's cloud environments through an exposed and vulnerable cloud instance resulting from a cloud misconfiguration. The misconfiguration was caused by a communication failure.

Two security measures were put in place by two teams, neither of which had knowledge of the other's actions. The development team had created a security network group, allowing public access to the vulnerable application. Meanwhile, the IT team had altered an overarching access control list (ACL) mechanism, which would have protected the exposed instance.

Lacking a centralized owner of cloud security operations within the organization allowed the two teams to make independent alterations to their security perimeter. The compromised cloud instance then allowed the CTAG to collect sensitive IAM credentials that gave them access to two of the organization's cloud platforms and resulted in the loss of sensitive data.

The following tactics are recommended to ensure that organizations maintain a secure environment for all teams.

- **Assign responsibility for all cloud operations** to a single organization entity, such as security operations or IT.
- **Develop a hierarchical organization structure** that includes cloud IT administration, DevOps, and security operations.
- **Implement change control policies** based upon the principles of CI/CD to ensure all cloud resources pass functionality, security, and accessibility requirements prior to production deployment.
- **Routinely scan all cloud infrastructure** to identify exposed cloud instances.

9. Ignoring Zero Trust Principles

Consider the ecosystem of controls available to an organization across the network, endpoint, cloud, application layer, and IoT. Identity management is the control linking these layers and, as such, IAM policies are the bedrock of a secure Zero Trust architecture.

But implementing Zero Trust isn't easy, and cloud threat actors view the burden of this difficulty as their golden ticket to your environment.

Identity is the new perimeter of your environment, making IAM the most critical factor to your organization's operation. Begin implementing the principles of Zero Trust architecture[11] within your IAM policies, roles and users. A strategic approach to cybersecurity eliminates implicit trust and continuously validates every stage of digital interaction.

If you're just starting your Zero Trust journey, the following tactics can give your organization a jumping-off point.

- **Architect cloud environments** using multiple cloud accounts designated for each organizational group or project.
- **Segment product and development cloud operations** within their own accounts. Should HR, IT, customer service, or marketing organizations require cloud resources, having their own cloud account operations will not affect other teams.

10. Failure to Establish Cloud IR Planning and Operations

Incident response (IR) plans are essential for organizations to properly recover from a breach or security incident. Cloud environments offer unique scenarios that need consideration when implementing a cloud IR operation.

Although costs to maintain a record of events taking place within your cloud environment can be high, you'll find cost-reducing solutions to cloud logging[12] with a little investigation. Properly implementing Zero Trust principles when designing IAM policies, roles, and users can be strenuous but will pay off significantly by reducing your threat landscape. Lastly, cryptojacking events are costly.[13] Monitoring cloud instances for indications of malicious activity will boost your ROI.

Tactics to help your organization establish a solid cloud IR plan include:

- **Define how cloud data is to be recorded and stored** to ensure adequate visibility into all cloud operations in the event of a security incident
- **Implement a robust quarantine control process** for all cloud resources in the event of a compromise. »

- **Mandate quarantine and security team analysis** of cloud resources—containers, VMs, serverless functions—in the event of a compromise. Compromised containers should never be restarted without a snapshot of their current operation.
- **Ensure adequate access** is given to the security research team responsible for investigating compromised cloud resources.

Closing the Gaps in Cloud Security

By addressing the top 10 cloud security risks, Unit 42 researchers believe the security of cloud environments can be dramatically improved, raising the bar for cloud security operations and allowing organizations to build manageable, well defended cloud environments.

For a comprehensive look at the current cloud security landscape, based on large-scale data and real-world attack scenarios, download Unit 42's Cloud Threat Report, Volume 7: Navigating the Expanding Attack Surface.

1. *Unit 42 Cloud Threat Report, Volume 7*, Palo Alto Networks, April 18, 2023.
2. *Unit 42 Cloud Threat Report, Volume 6*, Palo Alto Networks, April 12, 2022.
3. https://unit42.paloaltonetworks.com/atoms/
4. Shahar Fogel, "Logging Is Expensive And Static — Next-Generation Platforms Can Help," Forbes, February 9, 2022.
5. Paul Kelly, "Cybersecurity strategies: fighting alert fatigue and building resilience," Open Access Government, July 18, 2022.
6. *Prisma Cloud Administrator's Guide*, Palo Alto Networks, last revised August 1, 2023.
7. https://unit42.paloaltonetworks.com/atoms/
8. https://stix2.unit42.org/
9. *The State of Cloud-Native Security Report 2023*, Palo Alto Networks, March 7, 2023.
10. https://www.paloaltonetworks.com/prisma/cloud
11. https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture
12. Puneet Saraswat, "Cloud Logging Optimization - How We Saved Over $140k in Logging Costs," Harness, July 6, 2020.
13. William Gamazo, Nathaniel Quist, "PurpleUrchin Bypasses CAPTCHA and Steals Cloud Platform Resources," Palo Alto Networks, January 5, 2023.

Nathaniel Quist is manager of cloud threat intelligence for Prisma Cloud at Palo Alto Networks

Cybersecurity Consolidation – What It Is and Why You Should Care

By Lakshmi Kandadai

Global organizations face two major security challenges in today's business climate: digital transformation and macroeconomic conditions.

Let's address digital transformation. The past three years saw massive cloud IT investments and expansions, with organizations adopting large-scale remote and hybrid work to support business continuity. Cloud-based applications, devices and endpoints are more connected than ever. And as a result, organizations have a rapidly-expanding attack surface that opens them up to more cyberthreats.

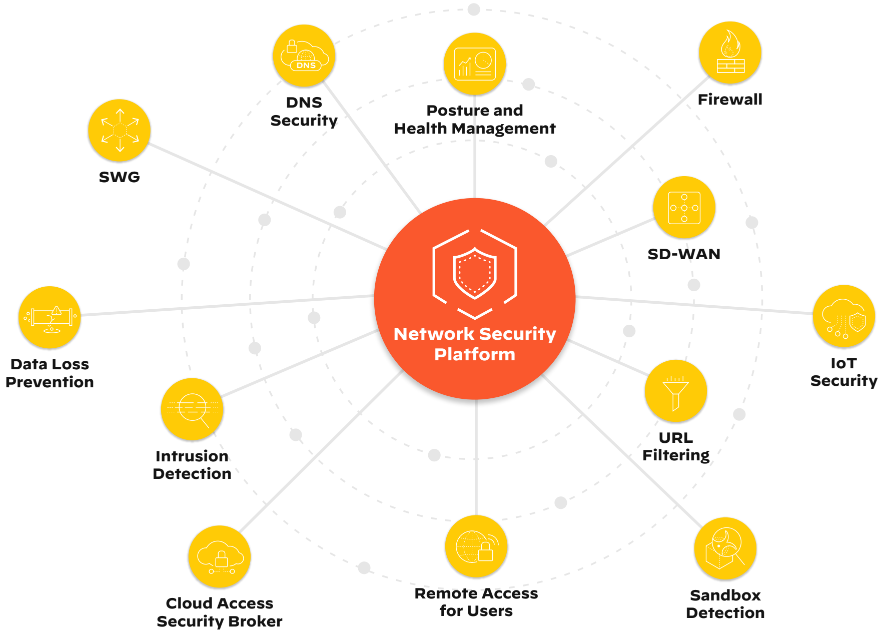
At the same time, economic uncertainty means that organizations are now tightening their purse strings – from scaled-back IT spending to re-evaluating current security tech stacks. Chief information security officers (CISOs) and security teams need solutions that reduce IT footprints while enhancing risk posture. In other words, solutions can do more with less.

So how can leaders defend against the evolving threat landscape while simplifying their security stack? Let's look at cybersecurity consolidation.

What Is Cybersecurity Consolidation?

Today's cyberthreats occur with more frequency and severity than in previous years. According to our global pulse survey of 1,300 C-Suite leaders in What's Next in Cyber 2022,[1] 96% of CXOs experienced at least one breach in the past year. The latest attacks target vulnerabilities in different networks, clouds and endpoints. They use tools like AI to bypass traditional cyber defenses used by organizations. »

Cybersecurity Consolidation



The usual reaction by security teams is to review and add products across the entire security spectrum – intrusion prevention, anti-malware, DNS security, WAF and more. Unfortunately, these point products seldom work together. Products from different vendors use different datasets, contexts, logging conventions and UIs, creating gaps and complexities in your security posture.

Cybersecurity consolidation combines multiple, siloed security functions into security platforms that manage your business risks by protecting your entire IT environment.

For example, organizations that use separate tools, such as intrusion prevention, anti-malware, DNS security and URL filtering, can choose a consolidated platform[2] that provides these protections together. The platform leverages shared intelligence to share information seamlessly across the platform, covering security gaps and giving teams the data and tools to respond faster to threats.

What Are the Benefits of Cybersecurity Consolidation?

1. Supercharge Risk Posture

The volume of mission-critical information for security analysts is reaching a tipping point. Today's threats use AI and automation to overwhelm defenders and exponentially increase response times. The information overload is simply too vast for security teams to handle manually.

A consolidated platform enhances risk posture by collectively sharing intelligence to prevent zero-day threats in real time. Tools share data points, dashboards and user experiences. They provide SOCs with a complete picture of their security posture. When every part of your cyber stack works together, they offer significantly better security.

2. Reduce Security Complexity

Large organizations employ 31.5 cybersecurity tools on average.[3] That's a lot of time, money and talent spent on managing the entire architecture. Add procuring and deploying future tools and vendors to the mix, as well as the additional training needed for security teams and users every time, and the security sprawl grows exponentially.

A consolidated platform reduces the number of vendors by integrating multiple tools and services, delivering them as a single, unified solution. From maintenance to software updates, to threat responses, all critical management requirements are fulfilled by a single vendor. The result is a highly scalable cyber infrastructure without needing additional resources.

Consolidated platforms also offer a single dashboard that provides visibility across all endpoints in your architecture. Security teams can access vital information, such as metrics and response times, from one location and reduce manual data sorting for security analysts.

3. Automate Security

In cybersecurity, speed is critical to detecting and mitigating threats. But, today's attacks overwhelm SOCs by using automation to target security gaps and silos. Analysts can spend days, weeks and even months chasing down false positives that lead nowhere. This means less time to spend on larger security projects and more opportunities for serious breaches.

Consolidated platforms leverage data across their systems to accelerate identification and response times. Platforms provide mission-critical data that give SOCs deeper actionable insights into threats, reducing manual workloads significantly. Security teams have more time to focus on larger threats, and organizations enjoy a much stronger security posture.

Why Should You Consolidate Your Security Now?

Cyberattacks on enterprises are growing in frequency and severity. Global cyberattacks increased by 38% in 2022, and business leaders are feeling the impact, according to our "What's Next in Cyber" 2022 report on 1,300 C-suite leaders: »

In the last 12 months

96%

of all respondents experienced at least one breach

57%

experienced three or more breaches

33%

of CISOs said they experienced an operational disruption as a result of a breach

84%

agree (to varying levels) that they have seen more security incidents due to hybrid work

The costs of inaction are...

Breaches guaranteed

96%

The percentage of organizations attacked in the last year

Source: Palo Alto Networks What's Next In Cyber

Operational disruption

33%

Of security professionals experienced operational disruption as a negative consequence of a breach

Source: Palo Alto Networks What's Next In Cyber

Financial and business impacts

$2.4M

The average cost associated with recovering from a breach

Source: Forrester

Almost every leader surveyed had experienced a breach, with over half experiencing three or more. And, the costs of inaction are high.

This doesn't include the damages to a reputation or regulatory compliance penalties that organizations incur when breaches happen. In fact, cyberattacks are at risk of becoming "uninsurable" as more organizations are impacted every year.

So where do you start with security consolidation? Here are three strategic areas to consider:

1. Managing Cyber Risks in Complex, Borderless Environments

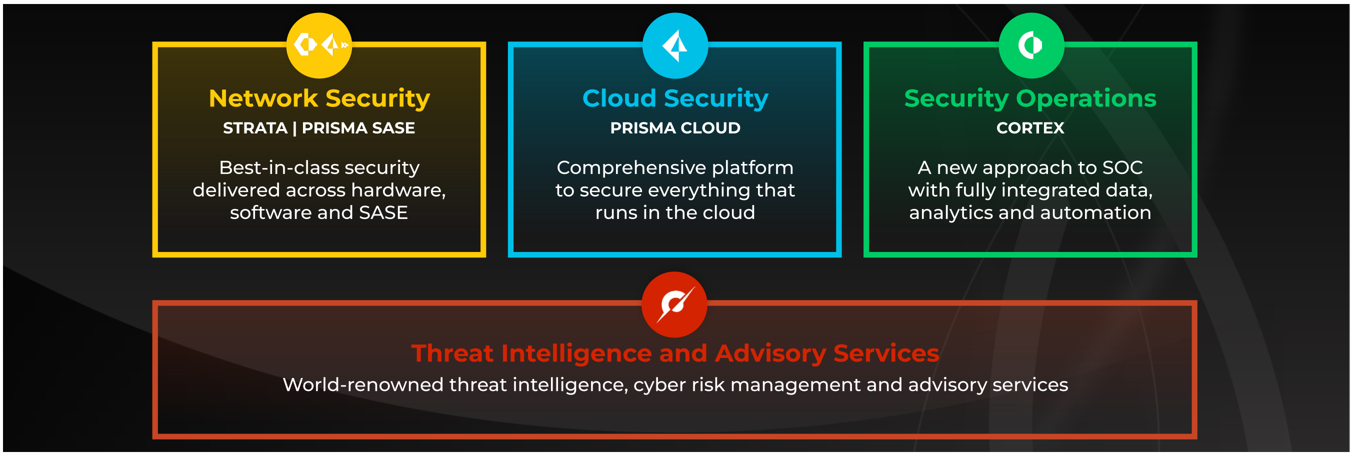
Securing across multiple clouds, data centers, hybrid locations and employees who connect from everywhere (both managed and unmanaged) is especially challenging. Multicloud networks are often overly permissive and depend on external-facing firewalls for protection, ignoring possible risks originating from within and enabling lateral threat movement. Furthermore, many traditional security tools are architected for on-premise environments. When extended or retrofitted to the cloud, they leave gaps that allow for excessive privileged access and permissions.

Enterprises with complex, multicloud environments should look for a provider that offers an end-to-end Zero Trust strategy.[4] You want a provider that understands your network's most critical data, assets, applications and services. They should apply those principles across all users, applications and infrastructure.

2. Maximizing Security Efficacy and Operational Efficiency

CISOs today face the unrelenting challenge of staying on top of cyberthreats while minimizing costs. After all, many business leaders still view cybersecurity as a cost center instead of an investment.

You'll want to look at how a provider helps you squeeze the most of every security investment. There are several key considerations when evaluating a cybersecurity provider: »



Network Security
STRATA | PRISMA SASE
Best-in-class security delivered across hardware, software and SASE

Cloud Security
PRISMA CLOUD
Comprehensive platform to secure everything that runs in the cloud

Security Operations
CORTEX
A new approach to SOC with fully integrated data, analytics and automation

Threat Intelligence and Advisory Services
World-renowned threat intelligence, cyber risk management and advisory services

- Look for integrated consoles for managing and monitoring consolidated platform(s).
- Look for the capability to automate threat response, allowing your SOC to focus on its highest-value tasks.
- Look for a vendor that minimizes the procurement process timeframe and costs, working with you to ensure a seamless transition.

3. AI-Driven Threat Detection and Response

Prevention is the gold standard for cybersecurity, but when a breach occurs, speed is everything. Security architectures built with multiple point products (mostly siloed and nonintegrated) can hinder response times significantly. Today's human-centered SOC is inundated by siloed data, with teams taking 287 days on average to identify and contain a data breach.

To ease the burden on security analysts, organizations need a provider that elevates their cybersecurity operations with AI-driven platforms. These platforms use security data gathered across their ecosystems to speed investigations and automate manual SOC tasks, such as eliminating non-essential threats.

For example, an extended detection and response (XDR) platform uses AI and machine learning to narrow down the hundreds of alerts SOCs receive every day. Analysts can then focus on the largest threats, which saves the organization time, money and personnel.

Palo Alto Networks: Your Partner for Cybersecurity Transformation

Cyber transformation is only possible when security leaders free themselves from legacy architectures. Security stacks built on point products result in gaps that leave enterprises vulnerable to attacks and ultimately cost more to resolve.

For organizations that want to simplify their security stack and maintain a best-of-breed approach, consolidation is key. Our next generation cybersecurity platforms provide end-to-end security from the data center, to the cloud, to your SOC.

Network Security – Our best-in-class Network Security Platform[5] across hardware, software and SASE secures the hybrid workforces and complex infrastructures of today.

Cloud Security – Our comprehensive cloud-native application protection platform (CNAPP)[6] secures DevOps from code to cloud, across multicloud and hybrid environments.

Endpoint Security – Our extended detection and response (XDR)[7] platform gives SecOps complete visibility into threats for lightning-fast investigation and response.

Incident Response – Our Unit 42[8] retainer services become an extension of your team, gaining a thorough understanding of your complex environment, so they can respond instantly to any breach.

Whether you already use Palo Alto Networks or are still exploring options for your organization, we want to help you make an informed decision. Learn more about cybersecurity consolidation:

- Consolidation: The secret to supercharging your SOC[9]
- Consolidation: How security platforms reduce implementation time and supercharge risk posture[10]

Want to know more about the Palo Alto Networks portfolio of platforms? Check out our cybersecurity solutions that work even better together.[11]

[1] "What's Next in Cyber: A Global Executive Pulse Check," Palo Alto Networks, December 13, 2022.

[2] https://www.paloaltonetworks.com/paloaltonetworks-portfolio

[3] "What's Next in Cyber," Palo Alto Networks.

[4] "What is a Zero Trust Architecture," *Cyberpedia*, Palo Alto Networks, last accessed August 16, 2023.

[5] https://www.paloaltonetworks.com/network-security/next-generation-firewall

[6] https://www.paloaltonetworks.com/prisma/cloud/cloud-native-application-protection-platform

[7] https://www.paloaltonetworks.com/cortex/cortex-xdr

[8] https://www.paloaltonetworks.com/unit42/retainer

[9] Niall Browne, "Consolidation: The Secret to Supercharging Your SOC," Palo Alto Networks, last accessed August 16, 2023.

[10] Haider Pasha, "Consolidation: How Security Platforms Reduce Implementation Time and Supercharge Risk Posture," Palo Alto Networks, last accessed August 16, 2023.

[11] https://www.paloaltonetworks.com/paloaltonetworks-portfolio#best-in-class

Lakshmi Kandadai is the director of product marketing, Cross-Portfolio and 5G Security at Palo Alto Networks

Consolidation: How Security Platforms Reduce Implementation Time and Supercharge Risk Posture

By Haider Pasha

Cybersecurity is one of the most complex landscapes organizations must navigate, with each new threat leading to more implementation, operation, and management complexity.

This is especially true for organizations that take a **point product approach** to their security. Implementing new security measures properly takes time and expertise. Every new tool must be installed, tested, and validated, and then employees must be trained to leverage them well.

But as organizations plan for a post-pandemic and digitally accelerated era, many CISOs across multiple industries strive for IT simplicity—with a focus on reducing their security vendor blueprint as part of their annual KPIs. In other words, fewer tools and vendors.

Implementation, in particular, has always been top of mind for successful cybersecurity programs because of the time, expense, personnel, and expertise often required to not only implement individual point products but to stitch them together to avoid security gaps while also eliminating redundancies.

In the event of a serious incident, SOC analysts typically confess to switching between multiple vendor consoles and event types in order to decipher alerts. Organizations and teams need a better approach so they're not either continually exposed or overworked by the alerts created by overlap.

How Do Cybersecurity Platforms Simplify Implementation?

By definition, a platform is the culmination of integrated points working as one system, such as integrated threat intelligence using automation and orchestration across a variety of security tools to take action against incidents in real time. This approach helps ease procurement, management, and operations of the cybersecurity stack while reducing cyber risk and improving security posture.

Deploying multiple products from different vendors typically requires a level of expertise beyond the capabilities of many in-house teams. Rather than “buying” implementation resources from consultants or cybersecurity services companies, organizations are looking for a more integrated approach to solutions implementation.

Benefits of cybersecurity platforms (versus point products):

- Reduce solutions' complexity and the number of integration points.
- Decrease deployment time and operational costs.
- Minimize risk of time and budget overruns.
- Consolidate security data lakes.
- Reduce the amount of practitioner and user training.

Cybersecurity platforms smooth and facilitate implementation while mitigating risks often associated with integrating point products in a seamless manner.

For example, as organizations evolve their cloud infrastructure, cybersecurity platforms **help reduce the number of vendors** required to secure multiple instances on the cloud, such as containers, serverless systems, and traditional virtual machines.

By binding the cloud security tools under one management system, the complexity of deployment—as well as the procurement process—means that customers are able to scale their cloud infrastructure much faster than before. This generally translates to cost savings in the form of faster security policy updates, incident management lifecycles, and reduction of alerts.

Another mission-critical implementation benefit to platforms is the ability to reduce the **cybersecurity skills gap**.[1] By consolidating all cybersecurity tools under the same architecture with easy integration and common connectors, organizations alleviate the need for armies of

»

technical staff—each with different certifications and experiences—to integrate new tools as the need occurs.

A Consolidated Approach

We chatted with several organizations that use our consolidated platform solutions. Here are their responses:

"Earlier on, we had at least four to six different integration points just for **firewalls**[2] and **endpoint security**[3] before we went with Palo Alto."

"Building security policy with fewer vendors is 3 or 4 times easier than upgrading a security policy for each different one."

"Having one ecosystem really does get a lot of efficiencies with integrations being so seamless."

Customers were also able to standardize and unify security policies and reduce their risk exposure due to the likelihood of reduced human errors. As a result, they've seen tremendous value in consolidating their security to a single vendor.

In fact, according to calculations made by Palo Alto Networks on customers' actual implementation costs, organizations can reduce total product costs by 19.4% by using a cybersecurity platform model for solutions implementation.

As organizations look for comprehensive solutions and services to secure the network, cloud, and endpoint and to optimize their SOC, our Palo Alto Networks portfolio of platforms offers the best-in-class set of capabilities along with leading third-party evaluations and efficacy tests and, together, deliver coordinated security enforcement across our customers.

What Is Cybersecurity Transformation?

Cybersecurity transformation is the implementation of a holistic cybersecurity strategy that incorporates risk management, incident response planning, threat intelligence, security governance, regulatory compliance, security awareness training, and more.

The fundamental concept behind cybersecurity transformation is to ensure that cybersecurity strategy is built into and aligned with every aspect of the business to facilitate digital transformation.

Why Is Cybersecurity Transformation Important?

Cybersecurity transformation has become an important investment area at a time when cloud security, hybrid work, artificial intelligence in cybersecurity, IoT security and other trends continue to alter the business landscape.

Traditional approaches to cybersecurity are not sufficient to meet the challenges of today's more sophisticated threat landscape. There is no longer a defined perimeter to protect, which means data, applications, networks, users, identities and devices are anywhere and everywhere:

- Across multiple cloud environments
- At distributed endpoints and edge locations across a company's network
- Wherever remote and hybrid workers happen to be located at any given time
- Wherever IoT devices are located

In other words, today's organizations are distributed, which creates larger and more diverse attack surfaces. This makes risk management, incident response planning, security governance, security awareness training, cloud security, network security and IoT security[1] more complex than ever.

The growing sophistication of adversaries exacerbates these challenges. According to Forrester in a study on data breaches in 2022,[2] "Even as companies strove to improve their security postures, enterprising attackers successfully made off with treasure troves of customer and citizen information."

The research shows that 74% of security decision-makers with responsibilities for network, data center, app security or security operations experienced at least one data breach at their firms in the prior 12 months, and 36% had three or more breaches.

The growing use of artificial intelligence (AI), machine learning[3] and automation is adding new challenges to an already complex environment, making cybersecurity transformation even more urgent. »

[1] Niall Browne, "Security Operations Center (SOC) Consolidation," Palo Alto Networks, last accessed August 17, 2023.

[2] https://www.paloaltonetworks.com/network-security/next-generation-firewall

[3] https://www.paloaltonetworks.com/cortex/endpoint-protection

Haider Pasha is the chief security officer of Emerging Markets for Palo Alto Networks

Intelligent tools enable adversaries to launch attacks that are both larger in scale and more targeted at specific vulnerabilities, such as IoT security, network security and remote workers.

Cybersecurity transformation helps organizations stay ahead of these threats by modernizing, integrating and consolidating all of the key aspects of a successful cybersecurity strategy—network and IoT security, cloud security, threat intelligence, IAM, SEIM, vulnerability management, multi-factor authentication, AI in cybersecurity.

Beyond that, cybersecurity transformation instills a culture of cybersecurity across the entire organization, including cybersecurity awareness training, incident response planning, compliance audits, security governance, cybersecurity frameworks and Zero Trust.[4]

4 Benefits of Cybersecurity Transformation

1. Reduce the Risk of Cyberattacks

Cybersecurity transformation offers improved risk management and protection against today's most pernicious threats. It sets the foundation for a future-proofed cybersecurity strategy as adversaries adapt and seek to exploit new vulnerabilities.

2. Simplify Security Architecture

Security teams today employ 31.58 tools on average,[5] each requiring time and resources for security experts to manage. Cybersecurity transformation and consolidation streamline the number of tools and services so defenders get maximum protection without the tool sprawl.

3. Move From Legacy Infrastructure to the Cloud

Many organizations still rely on legacy infrastructure (such as on-premise technology) that's inflexible and tough to scale. Cybersecurity transformation guides a company's journey from those legacy devices to cloud security, oftentimes with minimal disruptions to business operations.

4. Reduce Implementation and Procurement Time

One of the biggest challenges of adopting new cybersecurity tools is the time and resources spent on vetting, deploying and integrating those tools. With a solid cybersecurity transformation strategy, security teams can significantly speed up implementation and procurement time by evaluating assets, risks and solutions.

How to Implement Cybersecurity Transformation

Cybersecurity transformation typically requires a commitment from executive management in the C-suite and the boardroom because cybersecurity transformation affects security technologies, business processes and corporate cultures.

Steps to a successful cybersecurity transformation include:

- Commitment from executive management to develop a comprehensive cybersecurity strategy tightly aligned with digital transformation goals.
- Full assessment of current cybersecurity technologies and vulnerabilities. This includes risk management, regulatory compliance, cloud security, IoT security, network security, threat intelligence, IAM, vulnerability management, AI in cybersecurity, cybersecurity frameworks, etc.
- Engage with key stakeholders, including employees, executives, IT staff, SOC teams, and, when appropriate, customers and partners across supply chains and broader ecosystems.
- Engage with key technology partners in IT and cybersecurity.
- Prioritize and set goals, including timetables, budgets and risk management profile. Make sure to factor in regulatory compliance and compliance audits.
- Build a cybersecurity transformation roadmap and communicate regularly with stakeholders on progress, goals, timetables, etc.
- Conduct ongoing security audits and assessments.
- Measure results where possible in terms of improved risk management and KPIs such as speed to market or digital transformation successes.

Challenges and Barriers to Cybersecurity Transformation

Resistance to change. Implementing cybersecurity transformation is a major strategic undertaking. It involves a commitment to new security technologies and, in many cases, changing the corporate culture.

A shortage of cybersecurity talent and expertise. Given the industry-wide shortage of cybersecurity talent, business and IT leaders might believe they don't have the skills in-house to successfully effect cybersecurity transformation. Cybersecurity technology vendors and consultants can be helpful, but there may be additional costs involved.

The complexity of implementing new technologies. Organizations employ hundreds of cloud tools in the average workplace. Implementing new cybersecurity tools can potentially reveal integration difficulties when those tools aren't compatible.

Financial constraints and budget limitations. Cybersecurity transformation may require investments in new security technologies and training, both for SOC teams and general security awareness training across the organization. Unless management can be shown clear benefits in areas such as risk management or digital transformation, they may be hesitant to approve additional spending without a clear cybersecurity strategy and roadmap.

Future Trends in Cybersecurity Transformation

Cybersecurity is a perpetually moving target. As new vulnerabilities emerge—hybrid work, IoT and AI—adversaries adapt their tools and methods to exploit gaps.

Cybersecurity transformation provides a technological and cultural foundation for organizations to be faster, more efficient and more confident in adjusting to this constantly changing threat market. »

With cybersecurity transformation, organizations are better prepared to deal with both current challenges and future trends as they emerge and develop. These include:

- The growth of multicloud environments
- Hybrid and remote work
- Expanded and more tightly integrated digital supply chains
- IoT security
- Identity and access management (IAM)
- Artificial intelligence, including emerging tools such as ChatGPT and large language models (LLMs)

As advances in security technologies come to market, organizations that have undertaken successful cybersecurity transformation initiatives are well positioned to seamlessly incorporate innovations into the cybersecurity environments.

This has significant, positive implications for the business. Cybersecurity transformation facilitates a Zero Trust framework and leverages secure-by-design principles to embed cybersecurity strategy within the overall business strategy.

Business leaders can make decisions based on what they think is right for the organization, with the knowledge and confidence that cybersecurity risk management, regulatory compliance, security governance and other factors have already been factored into the process.

Cybersecurity transformation makes organizations more responsive to the needs of customers and employees and more innovative in developing new products, thus transforming cybersecurity from a potential limitation into a business enabler.

Attack Surface Risks, Challenges, and Changes

By Ross Worden

While digitization has simplified many organizational tasks, it has simultaneously made other facets of business more complex, including an ever-growing attack surface. As the number of connected devices and online services continues to grow, identifying all of these assets and potential vulnerabilities is a challenge. Implementing effective security measures becomes more difficult, especially if you are relying on manual inventory processes.

Depending on the company size, systems on the attack surface are responsible for creating millions or even billions of dollars in revenue. What's more, a failure in these systems could result in serious operational issues or even a complete shutdown. There's also the legal, regulatory and brand impacts. As such, it's vital that the availability of IT infrastructure components is fiercely protected.

What Attack Surface Challenges Do Organizations Face?

Digital Transformation

Transformation comes with many benefits, but these changes bring inherent challenges. For example, in a cloud environment,[1] multiple employees or third-party contractors might have the ability to intentionally or accidentally make a previously isolated end-of-life system publicly available online. Or, they could simply spin up a new cloud instance outside of security controls. These situations were rare with traditional IT infrastructures, but they're becoming increasingly common. »

[1] "What is IoT Security?," *Cyberpedia*, Palo Alto Networks, last accessed August 17, 2023.

[2] "Top Data Breaches And Privacy Abuses Exposed A Billion Records And Prompted $2.7 Billion In Fines In 2022," Forrester, February 27, 2023.

[3] "What is Machine Learning?," *Cyberpedia*, Palo Alto Networks, last accessed August 17, 2023.

[4] "What is a Zero Trust Architecture?," *Cyberpedia*, Palo Alto Networks, last accessed August 17, 2023.

[5] "What's Next in Cyber: A Global Executive Pulse Check," Palo Alto Networks, December 13, 2022.

Shadow IT / Rogue IT

Shadow IT (also called rogue IT) refers to situations where employees take IT infrastructure into their own hands to circumvent inconvenient policies, or to avoid the approval process. While they're typically well-meaning, they might inadvertently create attack vectors. For example, an employee may forget to take down a temporary website, provide an overly permissive IAM role for the sake of expediency, or even stand up a new cloud environment without informing IT and security teams.

If IT department and security team members don't know people are adding cloud workloads outside of governance, they won't know how to manage and monitor these attack vectors. These cases aren't entirely new occurrences, but cloud computing and adjacent innovations have certainly increased their frequency. According to the Unit 42 Cloud Threat Report, Volume 7,[2] more than 60% of organizations take longer than four days to resolve security issues, while threat actors typically exploit a misconfiguration or vulnerability within hours.

Remote Work

While many employees are returning to the office, there's no doubt that the remote work landscape has permanently expanded during the pandemic. Having employees work outside of the company network introduces a number of cybersecurity risks, including weaker security controls, increased susceptibility to threats and sensitive data passing through unsecured networks. We have seen a number of cases where threat actors gained access to corporate devices via an employee's insecure laptop.

How Is the Attack Surface Changing?

All of these challenges have an impact on the attack surface and overall attack surface management.[3] We see them exacerbated in key ways:

- **The Attack Surface Is Growing** – This is often driven by the increasing number of connected devices, systems and cloud instances, all providing cybercriminals with an ever-expanding range of potential vulnerabilities to exploit.
- **Systems Are Becoming More Fragmented** – Various departments use different versions of the same software. Some stay current on updates and patches while others don't, which leads to an environment that lacks stability and standardization.
- **Expanding Use of Networking Equipment** – VPNs are used as a protective component, but are often vulnerable to compromise. Meanwhile, data storage and analysis systems need to be accessible, but this leads to exposure to malicious actors and to the possibility that an employee inadvertently pushes sensitive information to a public dashboard. This can create massive regulatory and legal headaches even without a threat actor being involved.

How to Better Understand Your Attack Surface

The first step in understanding your digital attack surface is identifying all internet-facing assets that could potentially become a target for cybercriminals. This includes a comprehensive and continuously updated inventory of all assets, including their location, what software is installed, who has access (including third-party entities), who is responsible for that asset, and what security controls are in place.

Once you have identified all internet-facing assets, the next step is to conduct a comprehensive risk assessment. This involves identifying potential vulnerabilities and threats to each asset, as well as assessing the potential impact of a successful attack. Organizations can use a variety of tools and techniques to conduct an attack surface risk assessment, including vulnerability scanners, penetration testing tools and threat modeling. However, organizations must understand that all of these tools and techniques are only as good as the asset inventory you have.

Not all vulnerabilities are created equally, and organizations need to prioritize which vulnerabilities to address first, based on the potential impact of a successful cyberattack. Aside from assessing impact, you also need to consider the resources required to address vulnerabilities.

Attack Surface Reduction Strategies

Adequate protection requires a multi-faceted approach that involves reducing both the internal and external attack surface, as well as implementing effective security measures and attack surface reduction rules to address potential vulnerabilities. From malware to misconfigurations and ransomware attacks,[4] understanding the threat landscape is a critical first step.

One key issue here is remote desktop protocol (RDP), which represents almost one in four IT security problems according to our Attack Surface Threat Report.[5] While RDP is frequently used in organizations, it's often weakly authenticated and exposed to the internet, offering a host of opportunities to a potential attacker. It is a key attack vector for ransomware. »

Once security teams have identified and prioritized vulnerabilities, the next step is to roll out effective remediation measures to reduce your attack surface. These attack surface reduction rules might include limiting the exposure of certain assets, implementing access controls, applying security patches, deploying firewalls and intrusion detection systems, and conducting employee training on cybersecurity best practices.

Finally, it is critical to monitor your attack surface on an ongoing basis[6] and update your security measures as needed. A successful attack surface reduction strategy involves regularly reviewing your security policies and procedures, maintaining up-to-date inventories of all assets, and monitoring for new vulnerabilities and threats. Ongoing monitoring is especially important when underlying systems and processes may simply recreate previously patched vulnerabilities after they have been remediated.

Why Is Attack Surface Management Important?

Attack surface management (ASM)[7] is the process of identifying and managing all exposures and potential entry points to an organization's internet-facing IT systems. It involves taking a comprehensive approach to analyzing and mitigating potential vulnerabilities across an organization's entire attack surface: its networks, applications, data, employees and all exposures, including improper access controls on cloud instances and expired digital certificates.

Gone are the days when you could just assume that everything was in your on-premises environment, so it is essential to discover, evaluate and mitigate exposure of your internet-connected assets. Even as recently as 2022, we saw a significant jump in the portion of cloud issues[8] versus on-premises issues, compared to the prior year. Traditional vulnerability management solutions often struggle with out of date or incomplete asset inventories and are especially prone to failure in the cloud since most vulnerability management scanners[9] are IP-based and cloud IPs are constantly changing.

As such, attack surface management is more important than ever to identify potential vulnerabilities before they're exploited by cybercriminals. While conducting regular risk assessments and vulnerability scans, organizations can identify weak points in your security posture. These activities rely on having a comprehensive and up-to-date asset inventory.

These efforts serve to reduce the overall attack surface and lower the risk of cyberattacks and data breaches. This proactive approach to security helps improve brand reputation and avoid losses due to incident response[10] and downtime. It also helps organizations meet industry or government compliance requirements and avoid penalties or legal action, resulting from non-compliance.

Unit 42 Attack Surface Assessment

The Unit 42 Attack Surface Assessment can help you gain full visibility of your on-premise and cloud environments, giving you a comprehensive view of your IT infrastructure strengths and vulnerabilities.

Powered by our unmatched Cortex Xpanse solution,[11] plus Unit 42 security expertise and threat intelligence, we help you discover all public-facing assets vulnerable to CVEs and remediate threats before they can be exploited. Our attack surface management experts provide you with actionable, prioritized recommendations, and ensure you effectively prioritize actions.

The Unit 42 Attack Surface Assessment is an indispensable tool in your ASM program, helping you identify and manage exposure, mitigate risk and bolster your security posture now and in the future. If your organization needs help starting or advancing your attack surface management program, the Unit 42 Attack Surface Assessment can help.[12]

1. https://unit42.paloaltonetworks.com/category/cloud
2. *Unit 42 Cloud Threat Report, Volume 7*, Palo Alto Networks, April 18, 2023.
3. "What is Attack Surface Management?," *Cyberpedia*, Palo Alto Networks, last accessed August 17, 2023.
4. *2023 Unit 42 Ransomware and Extortion Report*, Palo Alto Networks, March 21, 2023.
5. *2022 Cortex Xpanse Attack Surface Threat Report*, Palo Alto Networks, July 19, 2022.
6. https://www.paloaltonetworks.com/cortex/cortex-xpanse
7. "What is Attack Surface Management ?, Palo Alto Networks.
8. https://unit42.paloaltonetworks.com/category/cloud
9. "A Vulnerability Manager's Guide to Attack Surface Management," Palo Alto Networks, October 21, 2021.
10. "What is Incident Response?," *Cyberpedia*, Palo Alto Networks, last accessed August 17, 2023.
11. https://www.paloaltonetworks.com/cortex/cortex-xpanse
12. https://www.paloaltonetworks.com/unit42/assess/attack-surface-assessment

Ross Worden is the senior consulting director of Unit 42 for Palo Alto Networks

Securing 5G for 2023 and Beyond

5G Is Designed to Go Places. Security Needs to Keep Up.

By Anand Oswal

While mobile technology has been around for decades, the current generation, 5G, is increasingly being recognized for the exciting new benefits it brings to enterprises, SMBs, and public sector organizations. Specifically, 5G capabilities such as ultra-high speeds, high availability, massive network capacity, and ultra-low latency, when properly secured, will support breakthroughs in digital transformation for new use cases such as private networks, network slice, and multi-access edge computing (MEC).

Organizations are drawn to 5G because of these new levels of reliability, performance, and connectivity. However, as 5G becomes how enterprises get work done, it places a greater emphasis on securing networks at all layers of the Open Systems Interconnection (OSI) model. For network operators, service providers, and equipment and solution providers, it's no longer enough to secure voice and data across Layer 3 (network layer) and Layer 4 (transport layer) of the pipe. We must secure up to and including Layer 7 (the application layer) to ensure that business continues on in this 24/7 environment. 5G is designed to go places. Security needs to keep up.

As this technology becomes pervasive across the globe, PwC has forecast that the global economic impact of 5G will exceed $1.3 trillion by 2030.[1] As organizations move to the next generation of connectivity, they will also need to confront potential new security risks. It's critical for any organization moving to 5G to integrate security as part of the deployment from the outset—understanding that 5G networks are the business today and not simply an enabler.

Why Protecting 5G Is Hard

5G is a major transformational technology that enables digital transformation of entire industry sectors and underpins entire economies. The proliferation of devices, the vast increase in intelligence at the network edge, and the aggregation of critical functionality at the network core bring challenges that together contribute to a perfect storm of security risk in 5G deployments. »

Security for previous generations of mobile technology was not focused on detecting and preventing attacks on all layers, all locations/interfaces, all attack vectors, and all software lifecycle stages. Because 5G finds its way into mission-critical applications that affect every aspect of public and private life, it's imperative to make sure that 5G deployments are protected by pervasive security that looks at all layers of the attack surface and provides controls to help mitigate risks. Enterprise-grade security enables organizations to take a Zero Trust approach to their 5G networks, including applying security on every level—down to the identification of every device, subscriber, and network slice.

Where Are the Emerging Threats from 5G Coming from?

Threats against 5G are likely to come from a few different vectors as attackers look to find the weakest link to gain access. 5G infrastructure involves multiple components, each of which represent an area where there is potential risk.

1. **Virtualized infrastructure**. 5G services will run on virtual machines (VMs) as well as Kubernetes-based container infrastructure in the cloud and in data centers. Threats against virtualization include denial-of-service attacks as well as misconfigurations, among others. There is also a risk of side-channel attacks, whereby an attacker is able to gain access to one piece of a virtualized infrastructure stack and then move laterally to exploit other connected elements.
2. **Network and management interfaces**. At the network layer, there is a risk from attacks against signaling and data interfaces. Attacks against these interfaces can include address spoofing, message tampering, and potential meddler-in-the-middle eavesdropping attacks.
3. **Application and service threats.** There are also risks from specific threats for applications and services. This includes advanced malware, command-and-control botnets, code injection, and application vulnerabilities.
4. **Radio rogues**. 5G is a wireless protocol and there is risk from rogue base stations in the radio access network (RAN) that can be used to attack the network.

As for emerging threats, we see the dataplane as a next potential battlefield. In the past, much of the security focus has centered on the signaling plane. However, given the expanded attack surface, it is becoming easier for adversaries to exploit vulnerabilities, API manipulation, and access controls, among others, on the dataplane, as well.

How Leaders Can Improve 5G Security

While there are emerging threats that organizations will face with 5G, there are also steps that can be taken to mitigate the risk.

1. **Adopt Zero Trust**. With a Zero Trust architecture, there is no notion of implied trust for the growing volume of devices and use cases on 5G. Instead, all devices and users are continuously validated in an approach that enforces least privilege across all the layers of the 5G stack.
2. **Embrace automation and AI**. The complexity of 5G deployments and the massive device connectivity will require faster and more repeatable approaches to deploying security. 5G security will be best served with an AI-powered approach that can identify devices and enable automated policy-driven approaches to reducing risk.
3. **Take a platform approach**. 5G is one part of a larger stack that organizations will deploy to enable applications. It's critical to take a unified approach to security that considers all attack vectors. A platform approach should also provide granular application identification policies and protection against advanced threats wherever they come from.

Designing Our Safe and Secure Journeys Together

5G represents a paradigm shift as organizations expand connectivity options to enable new capabilities. It also expands the attack surface with new interfaces and side-channel attack threats against virtualized network infrastructure. It's critical to consider the risks as part of a 5G initiative and integrate security as part of the deployment from the outset.

As organizations move to the next generation of connectivity, security can't be an afterthought. It's imperative to build security into 5G networks from the ground up. 5G security should be deployable on any cloud platform—private or public, across multicloud and multivendor environments, as well as on the service provider's 5G core network or at the MEC.

Advances like 5G can help us all go to places we've only dreamed but only if we work together to build in the safety and cybersecurity that will support that ride. Let's prepare for the journey together.

[1] "Health and social care to gain the most from 5G productivity and efficiency gains, which will add US$1.3 trillion to global GDP by 2030," PwC Global, February 2, 2021.

[2] Del Rodillas, "Securing the New Frontiers of Critical Infrastructure Networks," Palo Alto Networks, March 18, 2022.

[3] Leonid Burakovsky, Andre Ferreira, "Why Your Private 5G Network Needs An Enterprise-Grade Security Solution," Palo Alto Networks, June 21, 2022.

[4] "Breaking Trust: Building Sustainable Security for 5G with Zero Trust," February 25, 2022.

[5] https://www.paloaltonetworks.com/paloaltonetworks-portfolio

Anand Oswal is senior vice president and GM of Network Security at Palo Alto Networks

CRI Profile in Financial Services

By Lawrence Chin

Rising Cost and Complexity of Compliance

As the cyberthreats facing Financial Institutions (FIs) continue to grow, financial regulators have responded with updated and/or new regulations to address data protection, data security, cyber hygiene, third-party risk, and overall operational resilience. For FIs, this means a continuation of additional time, resources and costs being applied to meet regulatory requirements, which may be at odds with business growth and operational efficiency.

FIs that operate across jurisdictions face multiple, distinct and separate regulatory obligations and expectations. There may be nuanced differences across such a set of regulations, which further adds to the regulatory burden. To demonstrate compliance with these myriad regulations, FIs spend countless hours, devote significant people and technology resources to capture and provide evidence of appropriate processes and controls for each and every exam or audit.

However, there are often similarities across the required elements from these multiple exams as well. Instead of addressing these separately and repeatedly, the evidence collected to demonstrate compliance can be reused for similar obligations across multiple audits and jurisdictions.

Efficiency via Consolidation

Taking advantage of that concept, FIs can reduce the burden of responding to numerous separate exams using a consolidated approach to assess cybersecurity, resilience, and efficacy, with the help of the Cyber Risk Institute's (CRI) Financial Services Cybersecurity Profile ("The Profile").[1]

The Profile harmonizes over 2,400 regulatory expectations from around the world into 277 diagnostic statements (control objectives). This translation and consolidation addresses topical overlaps and phrasing differences to streamline and reduce the complexity of cyber risk and compliance activities for FIs. As an example, the Profile has a diagnostic statement (DE.CM-1.3) that calls for the implementation of intrusion detection and

»

prevention capabilities. After gathering the appropriate evidence once, a FI can re-use it satisfy similar obligations for the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, Payment Card Industry (PCI) Data Security Standard, European Central Bank (ECB) Cyber Resilience Oversight Expectations, International Organization of Securities Commissions (IOSCO) Guidance on cyber resilience for financial market infrastructures — just to name a few. Additionally, for the largest of FIs, the Profile has 49% fewer questions to address than another widely used assessment tool by this sector. Ultimately, the re-use of evidence and the smaller universe of diagnostic statements results in a substantial reduction in effort for compliance-related activities. Fewer interviews with assorted subject matter experts and less time are needed overall. Anecdotally, one FI cited a 35% average reduction in effort for their regulatory exams since adoption of the Profile.

Since the Profile may be used as a shared baseline for examinations by different financial regulators, this allows FIs to deploy their resources more effectively for compliance work, reduces time needed to reconcile exam issues, and makes security oversight easier. For the financial regulators, the widely adopted cyber control assessment framework in the Profile offers greater visibility into systemic risk across the financial sector and a common, consistent vocabulary as well. FIs have used the Profile with financial regulators in the Americas, Asia, and Europe too. Financial regulators or standards bodies that have recognized or acknowledged the Profile include the US Treasury, FFIEC, Federal Reserve Board, National Institute of Standards and Technology (NIST), IOSCO, European Union Agency for Cybersecurity (ENISA) and the Reserve Bank of New Zealand.

Evolution of the Profile

The CRI is a not-for-profit coalition of financial institutions and trade associations — currently with over 50 members which include the largest banking, financial markets and insurance firms, including regional and community banks and a growing base of global FIs. Working with its members, the CRI is responsible for curating and evolving the Profile to meet the needs of the financial services industry. Thousands of FIs have adopted the Profile — including some in the US that have transitioned away from the FFIEC Cybersecurity Assessment Tool (CAT). Outside of the US, where some firms are reluctant to use the NIST Cybersecurity Framework (CSF), the Profile provides a viable alternative.

As the CRI member and user base grows, the Profile is expected to evolve with cybersecurity-related standards for emerging technologies and practices (e.g., AI, cloud, privacy, financial digitalization and operational resilience. The CRI will update the Profile to reflect the changing regulatory environment, and plans to release v2.0 towards the end of 2023. If your firm has not considered using the CRI Profile yet, this may be a good opportunity to take a closer look and see how it may reduce the burden of your regulatory compliance activities and begin to explore the continuous controls monitoring and automation benefits.

Complement the Profile with Automation

With the Profile's consolidation of regulatory expectations down to 277 diagnostic statements, a FI can confidently re-use evidence for multiple exams or audits, which results in a significant time savings. However, the actual effort to identify, collect, and validate the needed artifacts and evidence for each diagnostic statement is still a manual process that is time- and resource-intensive. For many in the Risk and Compliance world, the gathering of evidence requires the most time and effort. To lighten that burden, automation and continuous controls monitoring can produce the desired evidence in real-time. Looking back at the use case for the diagnostic statement on intrusion detection and prevention, a network security management tool can generate a report of all intrusion detection and prevention system (IDPS) devices in the environment as evidence. Another example is a Cloud Security Posture Management tool that generates a compliance report for a FI's cloud estate against the Profile. With automation behind and aligned to the Profile's diagnostic statements, FIs can further reduce the effort required for exams and audits that encompass cybersecurity risks.

Connect today with Palo Alto Networks' Financial Services team to learn more on how we support the CRI Profile with enhanced automation and continuous controls monitoring to achieve measurable business impact for your risk, compliance and security teams.

Learn more about Financial Services Cybersecurity.[3]

[1] https://cyberriskinstitute.org/

[2] https://cyberriskinstitute.org/about/#Members

[3] https://www.paloaltonetworks.com/industry/financial-services

Lawrence Chin is a financial services security architect for Palo Alto Networks

ChatGPT: AI for Good or AI for Bad Camp

By Sean Duca

Science, technology, and all their components have strongly benefited humanity over generations. By definition, it is the search for new knowledge—so how could it be bad? But the reality is that every tool has the potential to be good or bad, and it depends on the people using it.

In our relentless quest to mimic and decipher the human mind, we have ushered in the era of artificial intelligence (AI). ChatGPT, a text-based AI bot, has become the latest tool making headlines for its viral use of advanced AI. From accurately fixing a coding bug and creating 3D animations to generating cooking recipes and even composing entire songs, ChatGPT has showcased the immense power of AI to unlock a world of incredible new abilities.

On the flip side, AI—as considered by many—is a double-edged sword. In cybersecurity, experts today have access to AI-powered security tools and products that enable them to tackle large volumes of incidents with minimum human interference. However, at the same time, amateur hackers can leverage the same technology to develop intelligent malware programs and execute stealth attacks at increasingly higher levels.

Is There a Problem with the New Chatbot?

Since the launch of ChatGPT in November, tech experts and commentators worldwide immediately became concerned about the impact AI-generated content tools will have, particularly for cybersecurity. A question many are asking is, "Can AI software democratise cybercrime?"

Recently, at the Black Hat and Defcon security conferences in Las Vegas, a team representing Singapore's Government Technology Agency[1] demonstrated how AI crafted better phishing emails and devilishly effective spear phishing messages—much better than any human actor could.

Using OpenAI's GPT-3 platform and other AI-as-a-service products, the researchers focused on personality analysis-generated phishing emails customised to their colleagues' backgrounds and individual characters. Eventually, the researchers developed a pipeline that groomed and refined the emails before attacking their intended targets. To their surprise, the platform also automatically supplied highly relevant details, such as mentioning a Singaporean law when instructed to generate content for their targets.

The makers of ChatGPT have clearly suggested that the AI-driven tool has in-built controls to challenge incorrect premises and reject inappropriate requests. While the system technically has guardrails designed to prevent actors using it for straightforwardly malicious ends, with a few creative prompts, it generated a near flawless phishing email that sounded "weirdly human."

How to Tackle the Challenges

As per the Australian Cyber Security Centre (ACSC), the total self-reported losses by Australian businesses hit with business email compromise (BEC) attacks reached $98 million in 2022, up from $81.45 million in 2021. This trend is only expected to rise with the availability of tools on the dark web for less than $10, the emergence of ransomware-as-a-service models, and AI-based tools such as ChatGPT, which collectively lower the barrier to entry for cybercriminals.

Considering the looming threats of an ever smarter and more technologically advanced hacking landscape, the cybersecurity industry must be equally resourced to fight such AI-powered exploits. However, in the long run, the industry's vision cannot be a vast team of human threat hunters sporadically trying to tackle AI threats with guesswork.

On the positive side, Autonomous Response is significantly used to address threats without human intervention, but the need of the hour is to take intelligent action to counter these evolving threats. While organisations can ensure a baseline level of cybersecurity by implementing practices such as the ACSC's Essential Eight mitigation strategies, it does not guarantee protection from newer, more advanced threats. As AI-powered attacks become a part of everyday life, businesses, governments,

»

and individuals must turn to emerging technologies such as AI and machine learning to generate their own automated responses.

Using AI Tools More Responsibly and Ethically

Following Australia's recent high-profile hacks, it's no surprise businesses are looking at ways to improve their cybersecurity posture. Implementing emerging technologies can no longer be ignored, especially with the Australian Securities and Investments Commission (ASIC) placing increased scrutiny on company directors who failed to prioritize cybersecurity.

However, businesses face a number of challenges in navigating the AI cybersecurity landscape. From technical complexities to the human components, there is a considerable focus, particularly on the balance between machines, the people involved, and ethical considerations.

Establishing corporate policies is critical to doing business ethically while improving cybersecurity. We need to establish effective governance and legal frameworks that enable greater trust that the AI technologies being implemented around us will be safe and reliable while contributing to a just and sustainable world. Therefore, the delicate balance between AI and people will emerge as a key factor in a successful cybersecurity landscape in which trust, transparency, and accountability supplement the benefits of machines.

Originally published in Australian Cybersecurity Magazine on January 18, 2023.

[1] Ben Wodecki, "Language models like GPT-3 could be used to send more believable phishing emails," AI Business, August 9, 2021.

Sean Duca is vice president and regional chief security officer for Palo Alto Networks

Healthcare Innovation: A Safe and Secure Approach

Six Focus Areas to Address the Top Security Challenges Facing Healthcare Organizations Today

By Jason Wessel

Digital innovation continues to improve patient outcomes and accelerate accessibility and equity of care while new digital technologies are empowering patients to engage in their care from anywhere. This profound transformation has enhanced the efficiency and productivity of healthcare professionals to make informed data-driven decisions, coordinate care more effectively, and ensure the continuity of care across multiple medical disciplines. Advanced analytics and AI tools help healthcare providers derive insights from vast amounts of valuable healthcare data. This enables evidence-based decision-making, personalized treatment plans, predictive analytics for population health management, and contributions to clinical research and innovations.

Healthcare IT organizations are now center stage and have a pivotal role in the digital healthcare delivery model. IT must ensure the availability of these digital systems and innovations to deliver care while not compromising patient privacy and the security of patient electronic health and personal data.

In conjunction with the ongoing digital transformation, care locations have undergone significant changes and expanded from the four walls of the acute care setting to ambulatory, telemedicine, and hospital-at-home care

»

settings. While these new care environments are optimizing patient-centric care delivery, they have significantly expanded the surface that needs to be secured by IT organizations.

Top Security Challenges of Healthcare Digital Innovation

Healthcare's digital transformation has created so many new opportunities, not only for patients and healthcare providers, but also for bad actors. Today, healthcare leaders need to think about:

Continuous Cybersecurity Threats

Due to the vast amount of valuable personal and medical data stored in healthcare providers' digital systems, cybercriminals are focused on profiting from data theft, life-threatening care disruption, and harassment of healthcare leadership and professionals and even patients through comprehensive attack campaigns. Top observed campaigns leveraged ransomware and supply-chain attacks against exposed and vulnerable systems and services. Phishing continues to be the most common attack vector used, enabling insider threats, both deliberate or unintentional.

Diversity of Connected Devices

Healthcare delivery organizations have the most diverse set of connected devices, which typically fall into three categories:

- **Devices managed by IT**, such as workstations, servers, laptops, printers, cameras, etc.
- **Devices managed by third-party business associates**, such as medical devices, building management systems, etc.
- **Unmanageable devices**, such as purpose-built fixed state devices that cannot be patched, legacy medical devices that cannot be decommissioned, etc.

Complete visibility of all connected devices and understanding their utilization is challenging due to the new distributed care environment. Even more challenging, implementing consistent preventative security controls to prevent security incidents across the diverse set of connected devices. This makes them a great entry point for cybercriminals to create catastrophic impact to the healthcare environment.

Distributed Applications and Workforce

The flexibility to enable the delivery of care from anywhere breaks established historical centralized security control models. Software as a service (SaaS), hosted applications, and public cloud-resident applications compound the issue with the centralized data center-delivered security stack architectures. To successfully leverage the digital innovations that enable delivery of care from anywhere,[1] there needs to be reliable connectivity and consistent distributed security controls that enable appropriate access to patient data, applications, and services.

Strategy for Safe and Secure Digital Healthcare Transformation

Security needs to be transparent and embedded in the process, enabling digital innovation instead of inhibiting it. Security must be proactive, preventive, and programmatic within a flexible architecture that enables the control of all users, devices, applications, and data regardless of location, while identifying and preventing known and unknown threats in an automated, contextual, data-driven, machine-led fashion. These six security focus areas help healthcare organizations achieve secure and safe digital transformation:

- **Implement a Zero Trust strategy**. A cybersecurity strategy must eliminate implicit trust and continuously validate[2] any established trust at every stage of their digital interactions through continuous security inspection.
- **Secure all connected devices**. Any connected device must be automatically identified; its communications, configuration, associated risk, and utilization continuously understood; and preventive security policies enforced that ensure the availability and security of all connected devices.
- **Enable care delivery from anywhere**. Enable healthcare professionals to securely access patient data and applications to deliver care through a secure access services edge (SASE) that ensures the best digital experience of the clinician and patient.
- **Protect all applications and data**. Consistent visibility and control of applications and data regardless of locations through a centralized set of security policies.
- **Ensure regulatory compliance**. Compliance should be continuously validated and achieved through an automated and proactive security approach.
- **Maximize integrations and automation**. Reduce security tool sprawl and focus on integrated security platforms that deliver automated outcomes. Automating security operations optimizes the use of constrained resources and eliminates analyst burnout.

Security should strengthen your digital transformation efforts, accelerate safe digital innovation, support delivering patient outcomes, and ensure the best experience for both the patient and healthcare professionals. Visit us at paloaltonetworks.com/healthcare to learn more.

[1] "Deliver Healthcare from Anywhere," Palo Alto Networks, February 28, 2023.

[2] "Zero Trust for Healthcare Organizations Overview," Palo Alto Networks, May 27, 2022.

Jason Wessel is a principal global healthcare solutions consultant for Palo Alto Networks

paloalto NETWORKS
UNIT 42
CORTEX BY PALO ALTO NETWORKS
UNIT 42 ATTACK SURFACE THREAT REPORT
EXPOSURE

2023 Unit 42 Attack Surface Threat Report

Executive Summary

Modern organizations are racing to update their enterprise network architectures to take advantage of Zero Trust security designs, cloud computing, software-as-a-service (SaaS) value delivery, and distributed workforces. This has fueled a dramatic increase of infrastructure, known and unknown, which in turn has greatly increased the complexity of securing their environments.

Exposures on publicly facing assets put them at risk of being compromised, and sometimes this leads to organizations becoming victims of opportunity as opposed to a targeted attack. Understanding what you need to protect is a precursor to any successful cybersecurity program — but companies and government agencies struggle to understand what they own and what services expose the most risk.

To put these sweeping changes into context and provide actionable intelligence, Unit 42 analyzed several petabytes of public internet data collected by Cortex Xpanse — the Palo Alto Networks attack surface management solution — in 2022 and 2023. This report outlines aggregate statistics about how attack surfaces worldwide are changing and drills down into particular risks that are most relevant to the market.

Key Findings

- **Constant change in the cloud creates new risk**. Cloud-based IT infrastructure is always in a state of flux. In a given month, an average of 20% of an organization's cloud attack surface will be taken offline and replaced with new or updated services. The deployment of these new services is generally responsible for nearly half of the organizations' new high or critical cloud exposures every month.

- **Remote access exposures are widespread.** Over 85% of organizations analyzed had Remote Desktop Protocol (RDP) internet-accessible for at least 25% of the month, leaving them open to ransomware attacks or unauthorized login attempts.
- **Cloud is the dominant attack surface.** A vast 80% of medium, high, or critical exposures belonging to the organizations analyzed were observed on assets hosted in the cloud.

Recommendations

- **Obtain continuous, comprehensive visibility:** Maintain a complete and up-to-date inventory of your organization's assets both on-premises and in the cloud to ensure consistent application of governance policies.
- **Transform your vulnerability mindset:** A lot of security breaches involve exposures due to issues such as misconfigured services, misconfigured firewalls, or even known vulnerabilities. Legacy vulnerability management processes fail to identify many of these issues, much less assist your organization in resolving them.
- **Enable your team to respond quickly to emerging threats:** When critical vulnerabilities arise, quickly understand your risk exposure for patch prioritization and mitigation of unpatchable end-of-life services.
- **Monitor remote access services:** Monitor all remote access points and usage to eliminate the risk of unauthorized logins.
- **Manage your attack surface at machine speed:** Attackers are utilizing automation to move at machine speed. It's critical that your organization is able to move at machine speed as well by leveraging attack surface management tools which provide proactive prioritization and enable automatic remediation of common exposures.

Your security teams face challenges in attack surface management, including understanding current threats, maintaining a comprehensive asset inventory to avoid unknown risks, and quickly addressing all risks on those assets. Any exposure or vulnerability in an internet-accessible system gives attackers an opportunity to harm your organization, causing downtime, data loss, financial setbacks, and potential brand reputation damage. By actively managing your attack surface, you proactively and automatically mitigate risks, staying a step ahead.

Scan the QR code to download the full report.

Don’t Panic.

Did you know? Coloring can help adults sleep better at night, reduce stress levels, calm their nerves, decrease anxiety, and even help pull them out of depression.

Protecting your organization can be stressful.
We’ve got you covered.