Securing the Future-Ready Organization

A modern strategy for holistic risk-based security

Security is a constant, ever-present challenge that never sleeps. Like rust, you have to stay ahead of it, otherwise the entire apparatus begins to disintegrate.

The last several years have challenged organizations to protect their digital assets and infrastructure from unauthorized intrusion and the inevitable fallout from successful attacks. With more of the business now dependent on IT services to drive growth and profitability, attacks on IT infrastructure present a higher degree of risk. If a critical service goes down, the business and its customers can suffer.

With a constantly evolving threat landscape, organizations need to continually adapt to emerging AI-assisted threats while meeting new business requirements through complex solutions such as hybrid multicloud architectures and securing remote workers and devices, which have made the attack surface more fluid and dynamic.

Acting reactively to issues of the moment, organizations haven't had much time to take a step back, take a holistic view of security, and understand the best leverage points in making it more effective. The problem, as we see it, is too much focus on technology and not enough on what can really drive a successful cybersecurity program, which is:

- Keeping up with emerging threats
- Having a strong governance, risk, and compliance (GRC) framework to drive consistent, compliant cybersecurity across the entire organization

In addition, clients should reduce their attack surface as much as possible and better understand its nuances so it can be appropriately protected. Organizations should also be able to measure and report on their security posture in terms of protecting against real threats. By aligning security programs with organizational goals, clients can achieve a more robust and effective security posture.

Governance, Risk, and Compliance as a Foundational Pillar of Modern Security

It's not uncommon for an organization to fall into the trap of identifying a problem within a specific team and impulsively purchasing a tool to address that isolated issue. The result is a proliferation of point solutions that may or may not address real risks.

Instead, organizations should take a risk-based approach to solving security issues with a strong foundation in GRC. Rather than viewing governance as bureaucratic overhead, it should be seen as the strategic vision that guides the organization's risk management efforts so that time and money are invested in areas that matter. By aligning security practices with business objectives and regulatory requirements, GRC ensures that security controls are implemented effectively and consistently across the enterprise.

From a GRC perspective, rather than investing in a new tool to address a specific risk, the best course of action is to communicate it to business partners and take action based on its threat profile — for example, does it pose a financial risk to the organization if exploited? Security investments and activities should flow from high-priority risks as identified in the risk register — the tool most

Case Study

Large Manufacturing Company

CHALLENGE:

Our client wanted to define their Zero Trust strategy in order to strengthen network security by verifying every user and device before granting access to authorized applications, regardless of location. Their goal was to minimize the impact of cyberattacks, enhance the protection of critical data, and improve operational efficiency. Additionally, they required a strategy that would ensure consistent security policies and user experiences for both remote and on-campus users while enhancing compliance and visibility.

HOW WE HELPED:

The Evolving Solutions Security Practice team conducted a two-day Zero Trust workshop. The workshop assessed the organization's Zero Trust maturity by examining the five core pillars: identity, devices, networks, data center/cloud, and data. With extensive expertise across all aspects of Zero Trust, the team developed a tailored roadmap to help the client achieve their objectives.

RESULTS:

Evolving Solutions delivered a Zero Trust Maturity Assessment, which provided an in-depth evaluation of the organization's strengths and areas for improvement across the five core pillars. The assessment assigned a maturity grade — ranging from traditional to optimal — for each pillar, providing a clear, structured roadmap for the client's Zero Trust journey to reduce cyberattack impacts, improve compliance, and enforce policies based on identity. The assessment also outlined prioritized next steps to help the client systematically advance their Zero Trust implementation.

organizations use to identify, evaluate, prioritize, and mitigate risks before they become problems.

When risks are not adequately communicated and tracked within a centralized risk register, opportunities to address priority items are missed. These overlooked risks can have far-reaching implications, potentially impacting the brand's reputation, disrupting production, or even leading to financial losses.

By basing security decisions on policy and risk, organizations can make meaningful improvements toward securing their brand and ensure that their actions are consistent with their risk appetite and strategic objectives. This programmatic approach to security, where risks are proactively identified, assessed, and mitigated, is essential for modern organizations operating in an increasingly complex and uncertain environment. Unintentionally, this is something that has gradually degraded in many enterprise organizations. Evolving Solutions aims to help its clients readjust back to taking a more programmatic approach to security.

Security as a Business Enabler

CFOs tend to view security as a cost center, largely because they lack an understanding of the direct relationship between security investments and their corresponding financial benefits. The cost of security should be weighed against the cost of not investing in it because brand damage and lost production can be very expensive. Security is not simply a cost to be minimized but rather a strategic investment that can drive business growth and success.

To better understand the business value of security, organizations should clearly articulate the potential repercussions of inadequate security, which can be quantified and presented as concrete consequences to the business's bottom line. In this way, security can be viewed as a business enabler rather than a cost center.

An example of security as a business enabler is the "shift left" approach, where security is built into applications during development instead of wrapping security around the application after development. In this way, organizations don't need to tool against security flaws inherent in applications. Once an application is released into production, the shift left mentality enables you to do business freely without fear that you're operating in a fractured security posture.

Moving Beyond Compliance to Proactive Security

Many organizations have taken a compliance-

first approach to developing a security program. Unfortunately, checking the compliance boxes without an overall strategy leaves many organizations vulnerable. Many publicized cases of compliant organizations have to deal with catastrophic breaches.

Using a holistic, risk-based strategy, organizations can protect their assets and check most or all of the compliance boxes at the same time. Evolving Solutions helps clients understand the steps and the motivations for pairing specific risk elements with meaningful solutions and services that are adaptive to the threat landscape. As new risks surface, your prior security investments can absorb and address the changes. The ultimate goal is to connect clients' risk registers with solutions and services that offer significant and relevant value.

Leveraging Predictive Detection and Future-based Visibility

Traditionally, SecOps has largely been reactive, focusing on responding to security incidents after they occur. However, the increasing sophistication and frequency of cyberattacks have highlighted the need for a more proactive approach. By leveraging automation and orchestration, organizations can shift from a reactive to a proactive security posture.

Working from a GRC-centered approach to security, organizations can explore tools designed to help security analysts develop a proactive approach to finding, assessing, and acting on risk mitigation before a vulnerability is exploited. Developing a proactive approach to security involves the ability to use predictive detection and future-base visibility to identify and get ahead of threats before they impact the organization. That can be done in a couple of ways.

1. **Security Information and Event Management (SIEM):** SIEM can be used for proactive risk analysis. SIEM aggregates log data and insights from various tools into a central repository where the information is correlated to identify and flag potential security threats and anomalies. For example, if a scan indicates that a group of servers poses a risk, security analysts can use that SIEM feedback to take action to protect the servers.
2. **Threat Intelligence:** Threat intelligence is open-source information about how threat actors are changing their tactics, procedures, and technologies to exploit vulnerabilities. The goal is to use automation and orchestration to take action based on known conditional risks, such as segmenting off a vulnerable section of the business from exposure. This can be done proactively using SIEM-based vulnerability scans and threat intelligence to identify and contain risks. The aim is to mature your toolset to enable the ingestion of external threat intelligence, parse it, and take advantage of it through hands-off automation.

Measuring Success

Organizations need to measure their success in identifying and handling risk, which is key to proving that security activities are actually delivering business value. Metrics drive better decision-making by providing an accurate understanding of the current state of the environment in terms of identity, network topology, and data alignment. From that, organizations can make more meaningful decisions and rely less on guesswork. So, when business decisions are made, whether about a purchase or a roadmap decision, it's based on the current state of the environment and risk profile.

There are two types of metrics to track:

1. **Dynamic:** Dynamic metrics measure progress on projects, such as changing your endpoint solution to a new vendor. A valuable metric for that is how many endpoints you have today that haven't been migrated to the new product. These metrics show the value or speed of achieving your "time to value" metric through specific actions or using a partner's services.
2. **Static:** Static metrics measure things that you're always concerned about—areas of risk that are monitored on an ongoing basis, such as capturing data from vulnerability scans or maintaining a list of items that are out of compliance or at risk.

Evolving Solutions works with clients to understand which metrics they should capture and automate the process of pulling metrics out of the environment and presenting the results in a dashboard that makes sense to an executive. We help organizations choose metrics that really matter to the business, are specific to the industry, or are specific to the client's toolsets.

Integrating Artificial Intelligence into Security

The Evolving Solutions Security Practice uses a two-part approach to harness the power of AI to enhance cybersecurity for predictive detection, optimized threat response, and to adapt to the evolving cybersecurity landscape.

Marketplace Tools

Evolving Solutions' technology partnerships give our clients access to cutting-edge technologies that can quickly process and analyze massive datasets to identify potential threats and vulnerabilities that would be impossible to detect manually. When evaluating potential partners and their tools, we select only those with a proven track record of success in accurately and efficiently identifying risks and attacks.

In-house Assessments

In addition, we have a proprietary process based on our own research and development for assessing a client's environment. Using these AI tools, we can rapidly ingest and interpret vast amounts of client data, including objective data like vulnerability scans and subjective data such as interview information. This process enables us to help clients develop a baseline characterization of their current state of affairs, using AI to parse that information, understand it, and respond accordingly in a very detailed fashion to proactively address vulnerabilities and strengthen their defenses. By combining these different types of data, our AI can paint a more complete picture of a client's security posture and identify potential risks that traditional assessment methods might miss.

Trends Shaping Next-Generation Security Operations

As cyber threats grow in sophistication and scale, organizations must evolve their security operations to stay ahead. Emerging trends emphasize a shift toward proactive defense strategies, leveraging automation, AI-driven insights, and a holistic zero trust approach to enhance resilience and agility.

Maturing Zero Trust

Looking ahead, we see organizations getting a better handle on implementing and using zero trust to secure information. While the concept of zero trust has been around for a while, organizations have been loosely interpreting and implementing it, often focusing on specific aspects like network segmentation or multi-factor authentication

Case Study

State Higher-Education Institution

CHALLENGE:

Our client was planning for growth in its cloud infrastructure to support centralized services for various campuses and institutions throughout the state. Their existing infrastructure was not originally provisioned to support this topology and expansion. They required new architecture to enable standardized security policies and shared services while streamlining operations and improving efficiency.

HOW WE HELPED:

The Evolving Solutions team implemented an hub-and-spoke virtual network topology with advanced firewall and DNS services in the hub. The solution included redundant security controls for traffic inspection and integration with load balancers to ensure failover and reliability. Our team's expertise in cloud networking and security enabled a seamless deployment with built-in redundancy and scalability.

RESULTS:

The institution now has a scalable, redundant security framework that supports future cloud expansion that can be integrated with and consumed by other campuses and institutions. The new architecture ensures a consistent security platform across both on-premises and cloud deployments, allowing team members to work with familiar tools and features while maintaining robust security policies.

instead of embracing the broader philosophy.

A true zero-trust architecture requires a holistic approach that encompasses continuous monitoring, real-time risk assessment, and adaptive access controls. This entails a deep understanding of the current state of the environment and the ability to leverage AI-powered tools to analyze data and identify potential threats.

Identity and Access Management

Identity and access management (IAM) plays a critical role in zero trust by managing user identities and access privileges. By implementing strong authentication mechanisms, enforcing least privilege principles, and continuously monitoring user activity, IAM can help prevent unauthorized access and mitigate potential insider threats.

By embracing continuous monitoring, AI-powered risk assessment, and adaptive access controls, organizations can move beyond traditional perimeter-based defenses and build a more resilient and agile security posture. This approach enables organizations to proactively detect and respond to threats, protect sensitive data, and maintain compliance with industry regulations.

Automation

Security orchestration, automation, and response (SOAR) platforms can be crucial in automating incident response, threat hunting, and compliance checks to reduce the burden on security teams and improve overall efficiency. SOAR helps organizations streamline security operations, enforce policies consistently, and discover shadow IT activities that might otherwise go unnoticed.

Evolving Solutions Security Practice

Evolving Solutions helps organizations understand their current state across the triad of organizational security: SecOps, GRC, and IAM. By evaluating existing processes, people, and technology, we deliver next-generation solution architectures and services recommendations ranging from assessments to tool optimization and integrations in order to accelerate time-to-value and enhance run-mode operational value.

By bridging disciplines and teams, Evolving Solutions focuses on shifting organizations from a reactive to a proactive security approach, providing the foundation needed to make it work in your environment. In the same way we help organizations transform IT operations, we can help you take a new approach to ensuring a safe and resilient environment for reliable business operations.

Let us show you how.

EVOLVING SOLUTIONS

Moving your organization from secure to safe.

Let's Get to Work!