OFFICE OF THE CTO REPORT

MODERNIZING IT:

Shifting Security to Risk Management

By Lori Mac Vittie
F5 Principal Technical Evangelist

Embracing a risk-based approach to security requires a significant shift in how we think about security and digital assets. But this shift is necessary given the rapid evolution of digital threats and the inability of existing security models to mitigate—let alone keep up with—them.

From Packets to Payloads to Processes

Traditional enterprise architecture frameworks were created without security in mind. It is absolutely true that security, in general, is an afterthought, having largely developed in a reactive model. That is, bad actors created attacks for which vendors and technology leaders built mitigations. This is due to the nature of digital transformation. In its earliest stages, the focus was on enabling productivity and efficiency through applications. These applications were largely fixed and static, residing in an isolated data center. There was little risk of attack from outside because there were no entry points into the data center until the era of the Internet dawned.

In its earliest form, security focused on protecting applications exposed on the Internet at the lowest layers of the technology stack: the network. Too many packets per second indicated some sort of denial-of-service attack. The security response? Firewalls capable of blocking the origin of the attack. Ports and protocols became the basis for security policies, with thresholds based on the volume and speed of packets attempting to use some application. The focus of security in this stage was to prevent disruption by cutting off an attack using simple, static rules.

Attacks evolved quickly in the face of a strong defense. As applications became richer and more capable, attackers quickly discovered vulnerabilities in software stacks. The industry began to see attacks embedded in the payload of messages exchanged between users and applications, each seeking to exploit some known vulnerability that would either cause an outage, offer unauthorized access, or exfiltrate data. The security industry again responded to these new forms of attacks, building solutions capable of detecting and neutralizing embedded attacks. The focus of security in this stage was to **detect and neutralize** attacks embedded in transactions.

As the digital economy expanded, reaching deeper and wider into every aspect of our lives, the opportunity for attackers also expanded. The value of data and access to consumer and corporate accounts is growing exponentially. Consider that an estimated thousands of video game accounts from the likes of Steam, EA Sports, and Epic "are stolen each month, with bulk account databases traded on private Telegram channels for sums between $10,000 and $40,000" (BitDefender). Today, account takeovers are rampant in every industry, from gaming to finance to healthcare to government services. During 2021, fraud cost the US government an estimated $87 billion in federal benefits (CNBC). The loss is primarily attributed to the pandemic unemployment program, which was largely operated via digital services.

The development of specialized bots that are designed to help consumers acquire one of a limited release of products is growing. These bots leverage technology and speed to ensure consumers can purchase a product online in less time than a human being can select the right size and color. Presented as a helper technology for consumers, these bots were nearly immediately leveraged by bad actors to quickly deplete resources for the purpose of resale at a higher price. Sneaker bots, grinch bots, and other specialty bots increasingly target specific high-demand products and suppliers.

"Thanks to resale sites like StockX and GOAT, collectible sneakers have become an asset class, where pricing corresponds loosely to how quickly an item sells out. Sophisticated sneaker bots, which can cost thousands of dollars, are key to creating the artificial scarcity that makes a sneaker valuable and, in turn, makes a brand seem cool."

New York Times

The security industry must now respond to attacks that target business processes, such as logging in to a service or purchasing products, in addition to existing attacks that target network services and applications. Traditional methods of inspection and evaluation are helpless to detect attacks against legitimate business processes. These are not vulnerabilities, nor are they subject to protocol exploits. These are processes exposed as a digital capability that is vulnerable to exploitation by those with the means to obtain—or money to buy—the right set of credentials.

The tools that protect the processes must also be able to differentiate between software and human consumers. This task is made more difficult by the reality that software (such as bots) is used both by consumers seeking efficiency and attackers seeking advantage. Security must evolve again, and this time it must shift toward risk management.

Embracing a risk management approach does not mean abandoning previous iterations of security. Indeed, attacks at every layer of the technology stack are constant and must be addressed. A risk management approach does not preclude the use of technologies to prevent volumetric attacks or those delivered by malicious content. A risk management approach does not focus on implementation details as much as it does on *how* threats are identified and risk is determined.

IF THE OBJECTIVE IS TO REDUCE ENTERPRISE RISK, THEN THE EFFORTS WITH THE BEST RETURN ON INVESTMENT IN RISK REDUCTION SHOULD DRAW THE MOST RESOURCES.

McKinsey

By approaching security with a risk-based mindset, organizations can move away from frenetic responses to attacks. Instead, they can deliberately make security decisions that align with business outcomes and consider the business's tolerance for risk.

The Evolution of Security Approaches

PREVENT	DETECT AND NEUTRALIZE	RISK MANAGEMENT
2000 - 2010	2010 - 2020	2020 -
Security focuses on preventing attacks by blocking ports, protocols, and IP addresses.	Security focuses on detecting and neutralizing attacks embedded in transactions.	Security begins to focus on assessing the risk/value balance of a given transaction.
• Security is primarily reactive.	• Security becomes proactive.	• Security shifts to risk management.
• Threats are identified based on packets.	• Threats are identified based on inspection that compares payloads against known vulnerabilities.	• Threats are identified by behavior and based on identity and asset.
• Controls are applied based on volumetric thresholds.	• Controls are applied based on detection of a threat.	• Controls are applied based on risk/reward profiles and the tolerance level of the business for risk.

Modernizing Security: Shifting Toward Risk Management

Today's digital enterprises connect with their customers and partners by delivering digital experiences mediated via modern applications. Therefore, the protection of applications is paramount to the task of modernizing security. These applications—and, at the next level of granularity, the workloads and services that are their building blocks—deliver value by creating, enriching, and/or providing access to the enterprise's digital assets in one way or another; they are therefore the central focus of a modern security mindset. Cybersecurity, as it is commonly referred to today, focuses heavily on the protection of the applications and APIs that expose those applications to connect users of all types to the digital assets that fuel a digital business.

Technology leaders are well aware of the tools and techniques required to implement reactive and proactive security. The question is: "How do you shift your organization to an approach based on evaluation of risk that relies largely on identity and assets?"

There are two core technologies central to this shift: authentication and access control. Authentication provides policies with the identity component, while access control provides governance of digital assets.

> **Authentication** is essentially the process of determining and verifying the identity of an application consumer. In the past, those were primarily humans seeking access to monolithic applications living in a private data center. As a result, all of the authentication systems and services could reside within that same data center. Today, modern applications use a distributed architecture and exposed APIs; therefore, authentication

must evolve. Authentication must now recognize not only human consumers, but also human proxies such as automated agents. In addition, because distributed applications are composed from services sourced from multiple clouds, authentication must exist in a world of federated, cross-enterprise identity stores. In short, while authentication is still a core element of basic defense, the expanded nature of today's digital services requires an evolved view of identity and how identity is validated.

Access control has been, and continues to be, the process of determining who—or what—can access an enterprise resource. But, as with authentication, the functionality required from access control has also evolved alongside enterprise applications. The first incarnations of access control were at the network layer; potential application consumers were either "inside" or "outside" a perimeter defined by network IP addresses. But today, with mobile consumers accessing distributed applications delivered across multiple delivery points, there is no neat, static perimeter to define the notion of inside versus outside. Therefore, access control must be couched in terms of the user identity, as validated by authentication. Modern application consumers can no longer be separated based on network location but are instead classified based on *their* identity.

These technologies, when combined with a complete inventory of all key digital assets, can be used to execute on decisions made with regard to the risk of allowing access to a given asset. Those decisions are based on an understanding of *how* those assets are exposed in conjunction with *who* those assets should—or should not—be exposed to.

Thus, the first step in modernizing security is to create or enhance the asset inventory with a focus on the means by which those assets are accessed and why. Additionally, technology leaders should keep in mind that applications are the primary means by which all data is accessed and therefore the inventory should also be able to map assets to those applications that interact with them.

Next, technology leaders will need to collaborate with business leaders to establish risk/reward profiles for key assets. The resulting risk/reward profiles should align security actions with business outcomes. For example, research from AiteNovarica tells us that "merchants lose 75 times more revenue to false declines than they do to fraud," making the risk of what is known as a false decline potentially outweigh the risk of allowing a transaction.

Therefore, interactions related to that transaction should be allowed or denied based on the organization's tolerance of risk. Factors that may influence the decision include the value of the transaction and the certainty associated with the legitimacy of the user. Is the system 50% certain the user is legitimate? More certain? Less? Each organization will determine its tolerance for risk and, based on that tolerance, adjust its profiles to apply security within those limits. A risk/reward profile guides humans and systems to determine how to address potential risk. More risk-averse organizations will tend to weight risk higher and apply controls to avoid it. Conversely, organizations with a higher tolerance for risk will rate reward as a larger factor in determining how to apply security controls.

The granularity here—that of evaluation at the transactional level—implies the ability to **continuously assess** digital interactions and adapt security decisions based on real-time context as assessed against policies. This approach is a key capability of zero trust approaches, as are the key technologies used to enforce decisions: authentication (who) and access control (what), as described in this white paper, “Zero Trust Security: Why Zero Trust Matters (and for More than Just Access).”

The ability to continuously assess digital interactions depends on an enterprise-level data and **observability** strategy—namely, that the organization has a strategy and is moving toward enabling full-stack observability plus a means to connect and correlate interactions across disparate stores if it’s not centralizing data in a single store.

Thus, a shift to risk management revolves around adopting three specific technologies: identity, observability, and access control with an overarching zero trust approach governing execution.

Modernizing IT Must Include Security

A key capability of a digital business is security—security of its digital assets, its data, and its customers’ financial and personal information.

In a digital business, nearly all interactions are conducted digitally, and thus security should become a first-class citizen of the business and, for IT, of the enterprise architecture. For most, this will mean evaluating the security practices, tools, and polices—many put into place in an ad-hoc fashion to combat rising attacks and emerging threats—with an eye toward whether they remain relevant in a primarily digital environment. A more deliberate, comprehensive approach will be necessary to fully secure all the digital assets and interactions required for the organization to thrive in a digital economy.

Many of the facets of operating as a digital business were not considered when organizations put their technology foundations into place in the form of an enterprise architecture. Security is one of those insufficiently considered facets.

As we hurtle toward a digital-as-default world, it is necessary for organizations to modernize IT to support and enable the rate of change and the data-driven decision making necessary to thrive in the future. A significant step is modernizing the enterprise architecture. That must include a more pervasive, comprehensive, and ultimately adaptive approach to security: a risk management approach.

To learn more about modernizing architecture—especially security—to serve a digital business, dive into our new O’Reilly book, “Enterprise Architecture for Digital Business.”