SECURITY TEAMS ARE OPTIMIZING FOR A WORLD THAT NO LONGER EXISTS

Most security tooling still assumes clear perimeters, static assets, and predictable access. Modern environments violate all three assumptions daily.

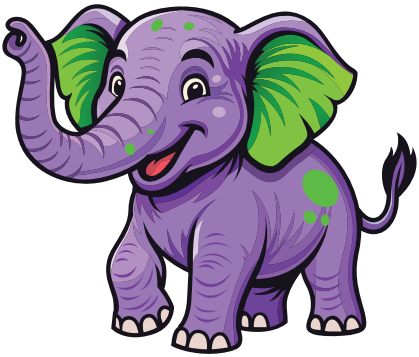
exactmarket℠

ELEPHANT IN THE ROOM EBOOK SERIES

TABLE OF CONTENTS

WELCOME TO THE ELEPHANT IN THE ROOM!

You have in your hands a guide designed to call out the elephant in the room. A topic that's too important to ignore but maybe isn't getting the attention it deserves.



INTRODUCING THE ELEPHANT

Security Teams Are Optimizing For A World That No Longer Exists

Security programs spend enormous effort maintaining controls designed for a different architecture. Firewalls still assume a network edge. Vulnerability scanners still expect a fixed inventory. Access policies still treat users as if they sit in one location, on one device, behind one gateway. None of that reflects how organizations operate today.

Cloud services spin up and retire in hours. Developers deploy infrastructure through code. Users authenticate from personal devices across dozens of SaaS platforms. Workloads shift between regions based on demand. The environment changes faster than the security model that governs it.

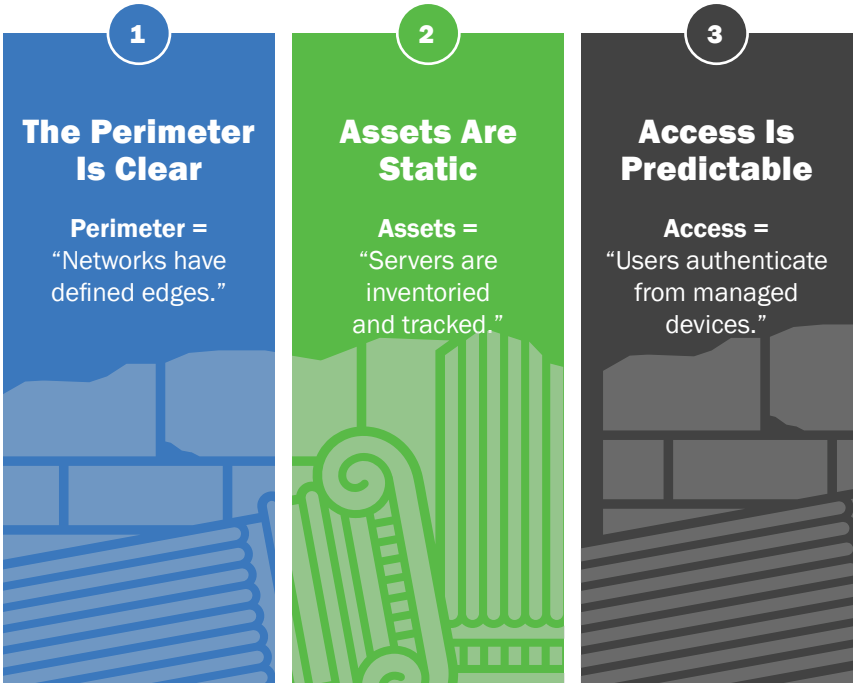
The result is not a lack of security investment. Organizations are spending more than ever, with global cybersecurity spending projected to reach $213 billion in 2025, up from $193 billion in 2024.[1] The problem is that much of that spending reinforces assumptions that stopped being true years ago.

This report examines the three foundational assumptions embedded in most security architectures, explains why each one has collapsed, and outlines a practical approach to realigning security operations with the environments they protect.

INTRODUCTION

The Three Broken Assumptions

Most enterprise security programs were built on three foundational beliefs:



These assumptions shaped decades of security architecture. Firewalls, intrusion detection systems, vulnerability management programs, and access control lists all rest on this foundation.

Attackers exploit the gap between how security teams think the environment works and how it actually works. A firewall rule protecting a data center boundary means nothing when the application moved to a SaaS platform two years ago. A vulnerability scan covering on-premises servers misses the workloads running in cloud environments that the asset inventory was never designed to track.

For many organizations, the security model has failed to evolve alongside modern infrastructure realities.

CHALLENGE

Assumption One: The Perimeter Is Clear

The Edge Dissolved. Security Didn't Follow.

The network perimeter was the original organizing principle of enterprise security. Everything inside the firewall was trusted. Everything outside was suspect. Security teams invested in deep packet inspection, IDS/IPS sensors, and DMZ architectures to control what crossed the boundary—but that boundary is gone.

What the Security Model Assumes	What Actually Happens
The network has a defined inside and outside.	Users, data, and workloads are everywhere. There is no "inside."
Traffic crossing the perimeter is inspectable.	95%+ of Chrome page loads use HTTPS. Decryption at scale breaks more than it finds.
VPN extends the trusted perimeter to remote users.	VPN grants broad network access from any device. It extends the attack surface, not trust.
Firewalls control access to sensitive systems.	Business-critical apps moved to SaaS. The firewall never sees the traffic.
Security tools monitor what matters.	IDS/IPS tuned for on-premises traffic misses cloud, API, and SaaS activity entirely.

Remote and hybrid work distributed users across home networks, coffee shops, airports, and co-working spaces. SaaS applications moved business-critical functions outside the data center entirely. Cloud infrastructure created elastic compute environments with no fixed address. And APIs connect systems across organizational boundaries continuously.

All that in mind, it's easy to see why the Cybersecurity and Infrastructure Security Agency (CISA) has stated that traditional perimeter-based defenses are no longer sufficient. CISA has directed federal agencies to adopt zero trust architectures that assume breach and verify every request regardless of network location.[2]

Yet many organizations still route traffic through VPN concentrators and apply firewall rules as if the perimeter is the primary enforcement point. According to research from Zscaler, 87% of all cyberthreats are now delivered over encrypted channels, rendering traditional perimeter inspection tools effectively blind to the majority of malicious traffic.[3]

Where the Gap Shows Up

The perimeter assumption creates specific blind spots that attackers exploit routinely.

SaaS applications operate outside network visibility

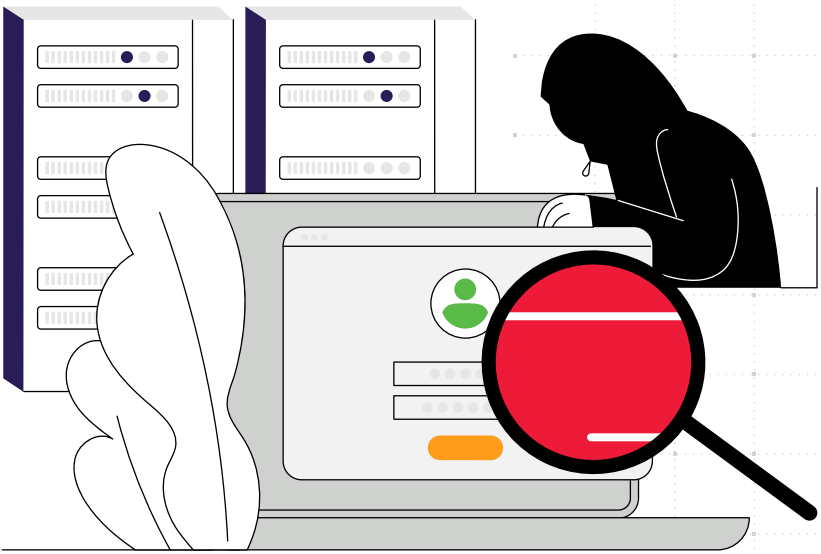
Business units adopt SaaS tools directly. Finance uses one platform, marketing uses another, and HR uses a third. Each application holds sensitive data and authenticates users independently. Network security tools never see this traffic because it never crosses the perimeter.

Cloud workloads have no fixed address

Infrastructure-as-code creates and destroys compute resources on demand. A server that exists at 9 a.m. may not exist at noon. Traditional asset-based security controls cannot track what they cannot inventory. The 2025 Verizon Data Breach Investigations Report (DBIR) highlights that attacks against cloud environments increased as organizations expanded cloud adoption without corresponding security controls.[4]

Encrypted traffic blinds inspection tools

The vast majority of page loads in Google Chrome now use HTTPS.[5] While encryption protects data in transit, it also means that deep packet inspection, a cornerstone of perimeter security, sees almost nothing useful without decryption and re-encryption at scale, which introduces latency, complexity, and privacy concerns.

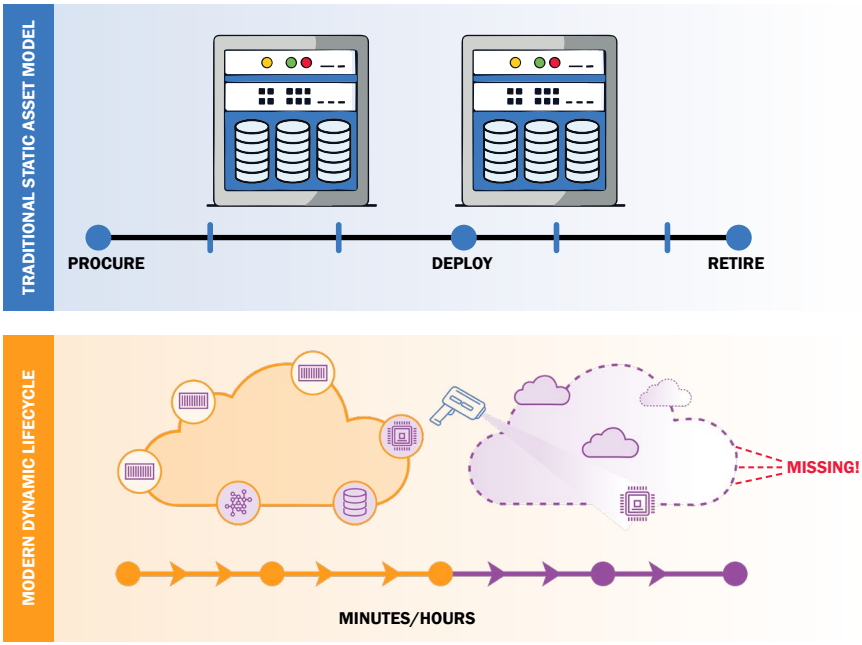


Assumption Two: Assets Are Static

The Inventory Problem

Vulnerability management depends on knowing what exists. Patch management requires an accurate asset list. Compliance audits assume organizations can enumerate their systems. Every one of these processes breaks when assets are no longer static.

Modern environments create and destroy infrastructure continuously. A Kubernetes cluster may spin up hundreds of containers in minutes and tear them down just as fast. Serverless functions exist only during execution. Cloud instances launch from templates and auto-scale based on load. Developer environments replicate production in temporary sandboxes.



The result is an environment where the asset inventory is outdated the moment it is compiled.

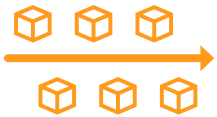
Research from Trend Micro found that 73% of organizations have experienced a security incident that exploited an unknown, or unmanaged, internet-facing asset.[6] The assets were not invisible because teams were careless. They were invisible because the operating model produces assets faster than governance processes can track them.

Three patterns of Asset Drift

SHADOW INFRASTRUCTURE

Cloud resources deployed outside governance, shown as hidden/ghosted servers.

EPHEMERAL WORKLOADS



Containers with short lifespans shown as appearing/ disappearing on a timeline.

ACCUMULATED TECHNICAL DEBIT

Legacy systems shown as old, dusty servers that nobody owns or monitors.

Shadow infrastructure

Development teams provision cloud resources directly to maintain velocity. These resources often bypass standard provisioning workflows. They may lack proper tagging, logging, or access controls. When a vulnerability is discovered in a widely used library, patching efforts miss the resources that do not appear in the official inventory.

Ephemeral workloads

Containers, serverless functions, and auto-scaled instances exist for minutes or hours. Traditional scanning tools operate on schedules: weekly, monthly, or quarterly. A workload that lives for 20 minutes will never appear in a monthly scan. Attackers understand this timing gap and target short-lived infrastructure precisely because it receives less scrutiny.

Accumulated technical debt

Legacy systems remain in production long after their intended retirement date. They run outdated operating systems, unsupported middleware, and unpatched applications. Nobody owns them clearly enough to decommission them, and nobody monitors them closely enough to detect compromise. These systems become persistent footholds for attackers who know they will not be disturbed.

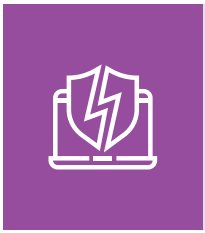
These patterns are not hypothetical. During a software licensing audit at a large global enterprise, the security team was forced to conduct deep network scans rather than relying on the existing asset inventory. What they found told the real story: a handful of Windows 2000 servers still running, several Windows Server 2003 machines that had never been updated past their original release, and hundreds of untracked test and development servers scattered across global offices. The Windows 2000 and 2003 systems were not forgotten experiments. They were running critical infrastructure. They had simply outlived every governance process designed to track them.

Assumption Three: Access Is Predictable

Nothing About Modern Access Is Predictable

Access control systems were designed for a world where employees worked from offices, used corporate-managed devices, and accessed a known set of applications through centralized directories. In that world, access patterns were stable enough to model, monitor, and enforce. That stability is gone.

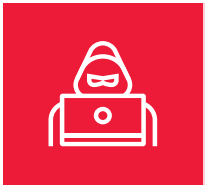
Users now authenticate from multiple devices across multiple networks to multiple applications throughout a single workday. Each access event has a different device posture, network context, and risk profile. No two sessions look the same, and access patterns that would have been flagged as anomalous five years ago are now routine.



Non-human identities compound the complexity. Machine accounts, service principals, API keys, and automation tokens now outnumber human users by ratios as high as 82:1.[7] These identities authenticate continuously, often with standing privileges and static credentials that never expire.

Large enterprises built through acquisitions inherit identity landscapes that no single team can fully map. Multiple Active Directories, cloud tenants stood up before governance frameworks existed, hundreds of service accounts created for projects that ended years ago, and service principals that outnumber the people who understand them. Nobody disables the old ones. The reasoning is always the same: “What if something breaks?” So they stay.

The human side is worse because it feels manageable but isn’t. Offboarding workflows disable the primary account reliably. But practitioners routinely find that secondary accounts, admin credentials, local accounts on vendor portals, and cloud environments provisioned for demos or proofs of concept survive long after the person leaves. One forgotten cloud environment can run for years, accumulating costs, because no one is watching the bill closely enough to question it and no one remembers who built it. ISP management portals, CI/CD tokens, SaaS admin accounts: if they are not explicitly linked to the primary identity in the deprovisioning workflow, they survive indefinitely.



The 2025 Verizon DBIR reports that credential misuse remains responsible for 22% of all breaches and 88% of web application breaches.[8] Attackers do not need exploits when they can log in.

The Consequences of Unpredictable Access

Static policies cannot match dynamic behavior

Role-based access controls (RBAC) assign permissions when a user joins or changes roles. Those permissions accumulate over time and are rarely reviewed. The gap between what a user needs and what a user has grows wider every quarter. Attackers who compromise an over-permissioned account inherit every excess privilege.

In practice, most access reviews are rubber-stamped. Managers approve what they approved last quarter because reviewing 200 entitlements line by line takes hours they don't have. Modern identity governance tools can flag when someone has changed departments, moved into a new reporting structure, or holds entitlements that no longer match their role. But those tools only help if the review process is built to act on what they surface, and most aren't.

Detection tools assume baselines that no longer hold

User and entity behavior analytics (UEBA) build behavioral baselines to detect anomalies. When users work from unpredictable locations on varying devices at irregular hours, the baseline itself becomes unreliable. The result is either excessive false positives that overwhelm analysts or loosened thresholds that let real threats pass unnoticed.

MFA is not the safety net it was assumed to be

Multi-factor authentication (MFA) reduces risk from stolen passwords, but it does not prevent token theft, session hijacking, or adversary-in-the-middle attacks that capture authenticated sessions. Attackers increasingly target post-authentication tokens rather than credentials themselves. Once a session token is stolen, the attacker inherits a fully authenticated session that bypasses MFA entirely.

In most organizations, predictable access was a product of a controlled environment. That control is largely gone.

The Compounding Effect

When All Three Assumptions Break Simultaneously

Each broken assumption creates risk on its own. Together, they compound.

COMPOUNDING RISK CASCADE

A dissolved perimeter means threats arrive through channels that security tools do not monitor. Static asset models mean those threats land on systems that security teams do not know exist. Unpredictable access means the compromised identity behaves in ways that detection tools cannot distinguish from legitimate use.

The 2025 IBM Cost of a Data Breach Report found that breaches involving stolen or compromised credentials cost an average of $4.67 million and took an average of 246 days to identify and contain.[9] That extended dwell time is the logical outcome of systems optimized to find threats in an environment that no longer exists.

$4.67M

Average cost per credential-based breach in 2025[9]

246 DAYS

Average time to identify and contain breaches involving stolen credentials[9]

TRANSFORMATION

Rebuilding Security for the Actual Environment

The Shift in Thinking

Fixing this does not start with buying new tools. It starts with accepting that the operating model has changed and that security architecture must follow.

For years, security was additive. When a new risk appeared, teams added a new tool. New attack vector? New sensor. New compliance requirement? New audit process. This approach worked when the environment was stable. In a dynamic environment, adding more tools to an outdated model increases complexity without improving outcomes.

According to a joint study by IBM and Palo Alto Networks, organizations now deploy an average of 83 security tools from 29 different vendors.[10] More tools have not produced better outcomes. They have produced more alerts, more dashboards, and more fatigue. A 2025 Sophos cybersecurity survey found that 76% of IT and cybersecurity professionals report experiencing burnout over the last year.[11]

In practice, security teams inherit tools from predecessors, add tools to satisfy auditors, and keep tools running because removing them feels riskier than maintaining them. The stack grows in one direction. The most visible example is the endpoint. It was not unusual to find seven or more agents running on a single workstation: antivirus, process monitors, deployment tools, DLP agents, and more, most of them overlapping in capability. Endpoint protection platforms have consolidated some of that sprawl, but the pattern repeats at every layer of the stack. Each tool made sense when it was purchased. Nobody ever asked whether the previous five still did.

The transformation required is architectural, not incremental. Security must move from protecting a static perimeter to continuously validating trust across a fluid environment.

83
security tools deployed on average[10]

29
different vendors per organization[10]

76%
of cybersecurity professionals report burnout[11]

Three Shifts That Matter

For years, teams treated identity as a supporting function—necessary, but largely invisible. That assumption no longer holds. In modern environments, identity determines how applications run, how data is accessed, how incidents unfold, and how organizations show resilience under regulatory scrutiny.

Many organizations still treat identity as routine IT work. In practice, it now affects performance, risk, compliance, and incident response. A compromised identity can cross cloud boundaries, bypass network controls, and access data directly. A shift in thinking reshapes identity's role across three areas: daily operations, threat detection, and regulatory accountability.

From perimeter enforcement to identity-centric security

When the network edge is no longer the primary enforcement point, identity becomes the consistent control layer. Every access request, whether from a human user, machine account, or API call, must be evaluated based on who is asking, what they are asking for, and whether the context is appropriate. This is the core principle behind zero trust architectures, which CISA, NIST, and the U.S. Department of Defense have all adopted as standard.

From periodic scanning to continuous asset discovery

Monthly vulnerability scans cannot keep pace with environments that change hourly. Security teams need continuous visibility into what exists, where it runs, and how it connects to other systems. This requires integration with cloud APIs, container orchestrators, and infrastructure-as-code pipelines to detect assets as they appear, not after they have been running unmonitored for weeks.

From static policies to adaptive access controls

Fixed RBAC policies fail in dynamic environments. Access decisions must incorporate real-time signals: device posture, network location, time of day, behavioral patterns, and risk score. When context changes, access decisions should change with it. Just-in-time privilege elevation replaces standing administrative access. Continuous evaluation replaces one-time authentication.

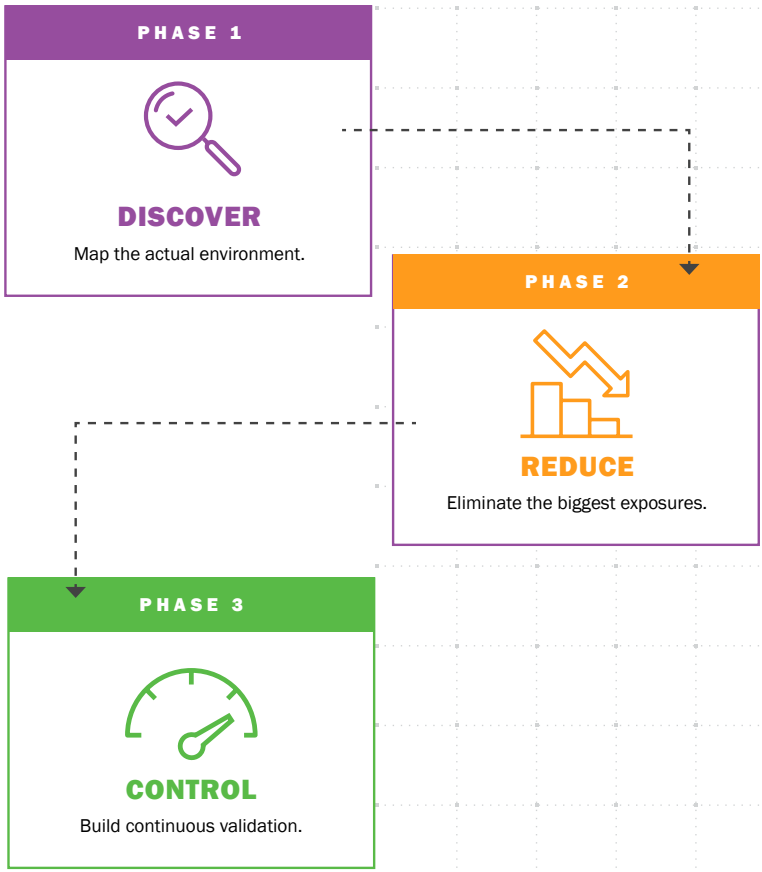
SOLUTION

The Security Realignment Playbook

Closing the Gap Between Model and Reality

Security realignment is not a single project. It is a structured progression that maps the real environment, reduces the exposure created by outdated assumptions, and builds controls that adapt as conditions change.

This playbook follows three phases: Discover, Reduce, and Control. Each phase addresses specific gaps created by the three broken assumptions and builds the foundation for the next.



PHASE 1

Discover (Map the Actual Environment)

Most security programs operate on incomplete information.
The discovery phase replaces estimates with facts.

MAP THE REAL ATTACK SURFACE

Inventory every asset, identity, and access path across on-premises, cloud, SaaS, and edge environments. Include ephemeral workloads, machine identities, and shadow infrastructure. Traditional CMDB entries are not sufficient. Connect to cloud provider APIs, container registries, and identity platforms to build a live picture of what exists now, not what existed at last audit.

IDENTIFY ASSUMPTION GAPS

Compare current security controls against the actual environment. Where does the firewall policy reference network segments that no longer carry sensitive traffic? Which vulnerability scans miss cloud-native workloads? Which access policies grant permissions based on roles that no longer reflect how people work? Document every gap between the security model and operational reality.

ESTABLISH COMMUNICATION SURFACE VISIBILITY

Map how data flows between systems, users, and external parties. This includes API connections, SaaS integrations, collaboration tools, and automated workflows. Attackers follow data paths. Security teams must see those paths clearly to defend them.

PHASE 2

Reduce (Eliminate the Biggest Exposures)

Once the environment is visible, reduce the attack surface created by outdated assumptions. Focus on the exposures that move the needle first.

RETIRE CONTROLS PROTECTING BOUNDARIES THAT NO LONGER EXIST

Firewall rules for decommissioned network segments, VPN configurations for office-only access models, and IDS signatures tuned for traffic patterns that shifted to the cloud-all consume resources without reducing risk. Removing them is honest.

CONSOLIDATE IDENTITY AND ACCESS

Get rid of dormant accounts, stale permissions, and standing administrative privileges. Enforce least privilege across human and non-human identities. Right-size cloud IAM policies that were configured broadly during initial deployments and never reviewed. This directly reduces the attack surface that credential-based attacks exploit.

CLOSE THE EPHEMERAL ASSET GAP

Integrate security controls into the deployment pipeline so that containers, serverless functions, and auto-scaled instances are scanned and configured before they run, not after. Shift-left approaches embed security into CI/CD workflows, catching misconfigurations and vulnerabilities at build time rather than in production.

PHASE 3
Control (Build Continuous Validation)

Reduction is only effective when followed by controls that adapt to ongoing change.

IMPLEMENT CONTINUOUS ASSET DISCOVERY

Replace scheduled scans with always-on discovery that detects new assets, configuration changes, and exposure as they happen. Integrate with cloud APIs, Kubernetes controllers, and infrastructure-as-code systems to maintain an accurate, real-time picture of the environment.

DEPLOY ADAPTIVE ACCESS CONTROLS

Replace static RBAC with policies that evaluate context at every access decision. Device posture, network location, behavioral patterns, and risk signals should all factor into whether access is granted, challenged, or denied. Just-in-time privilege elevation should replace permanent administrative access. Sessions should be re-evaluated continuously, not just at login.

ALIGN DETECTION TO IDENTITY AND BEHAVIOR

Move detection capabilities from network-centric models to identity-centric models. Monitor how identities behave across systems, not just whether traffic crosses a boundary. Correlate activity across cloud platforms, SaaS applications, and on-premises systems to detect lateral movement, privilege escalation, and data access anomalies that network sensors would never see.

MEASURE AND ADAPT QUARTERLY

Track metrics that reflect alignment, not just activity. Useful metrics include percentage of assets covered by continuous discovery, percentage of identities operating under least privilege, mean time to detect identity-based threats, and reduction in standing administrative privileges. Review quarterly and adjust controls based on how the environment has changed.

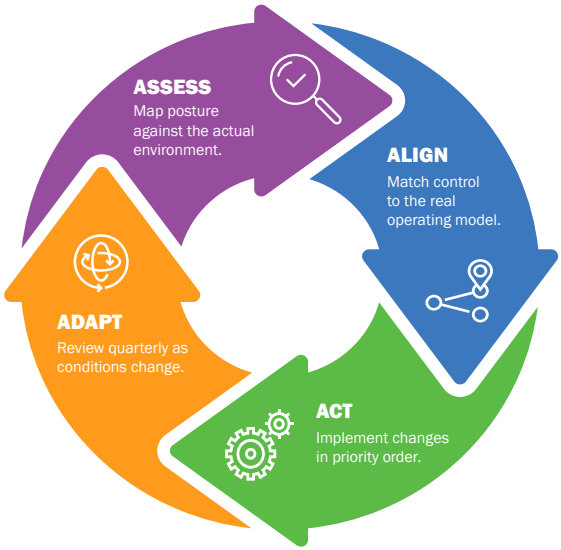
The 4A Security Decision Framework

A Strategic Sequence for Realignment

This framework provides a repeatable decision model for security teams navigating the shift from assumption-based to evidence-based security.

Security Decision Framework

Continuous cycle of evidence-based security decision making.



Assess

Map the current security posture against the actual environment. Identify where controls protect boundaries, assets, or access patterns that no longer reflect reality. Quantify the gap between the security model and operational truth. Prioritize by exposure, not by legacy investment.

Align

Match security controls to the real operating model. Determine which workloads require identity-centric protection, which assets need continuous discovery, and which access patterns demand adaptive enforcement. Align security investments with where risk actually accumulates, not where it accumulated five years ago.

Act

Implement changes in priority order. Remove outdated controls that consume resources without reducing risk. Deploy continuous discovery and adaptive access. Embed security into deployment pipelines. Consolidate identity governance. Each action should be documented and measurable.

Adapt

Review quarterly. Cloud environments change weekly. SaaS adoption accelerates monthly. Threat actor techniques evolve continuously. Security architecture that remains static will drift out of alignment just as the previous model did. Build adaptation into the operating rhythm, not as a response to incidents.

GLOSSARY

TERM	DEFINITION
adaptive access control	Access policies that evaluate real-time context, including device posture, location, behavior, and risk score, before granting, challenging, or denying access.
asset drift	The gap between an organization's official asset inventory and the actual infrastructure running in production. Caused by cloud elasticity, shadow IT, and ephemeral workloads that outpace governance processes.
assumption debt	The accumulated risk created when security controls continue to enforce models that no longer reflect the operating environment. Grows silently and compounds over time.
attack surface	The total set of points where an attacker could attempt to enter or extract data from an environment, including cloud workloads, SaaS applications, APIs, and machine identities.
continuous discovery	An approach to asset management that detects new resources, configuration changes, and exposures as they occur rather than relying on scheduled scans. Integrates with cloud APIs, container orchestrators, and infrastructure-as-code systems.
ephemeral workload	A compute resource, such as a container, serverless function, or auto-scaled instance, that exists for a limited time. Traditional security scanning cannot reliably detect or assess ephemeral workloads due to their short lifespan.
identity-centric security	A security model that treats identity as the primary enforcement point rather than the network perimeter. Every access request is evaluated based on who is requesting, what is being requested, and whether the context is appropriate.
just-in-time (JIT) access	A method of granting elevated access only when needed and automatically removing it after the task is complete. Reduces long-lived privileges.
machine identity	A non-human identity used by applications, scripts, services, automation tools, or cloud workloads to authenticate and access resources. Machine identities often outnumber human accounts.

TERM	DEFINITION
permission creep	The progressive misalignment between an organization's security architecture and its actual operating environment. Occurs when infrastructure evolves faster than the security controls governing it.
shadow infrastructure	Cloud resources, SaaS applications, or development environments provisioned outside standard governance processes. Often lacks proper security controls, monitoring, and access management.
shift-left security	The practice of integrating security controls earlier in the software development lifecycle, typically into CI/CD pipelines, so that vulnerabilities and misconfiguration are caught during build rather than in production.
zero trust	A security model that assumes no identity or system is trusted by default. Access is continuously verified based on context, behavior, and risk.

CITATIONS

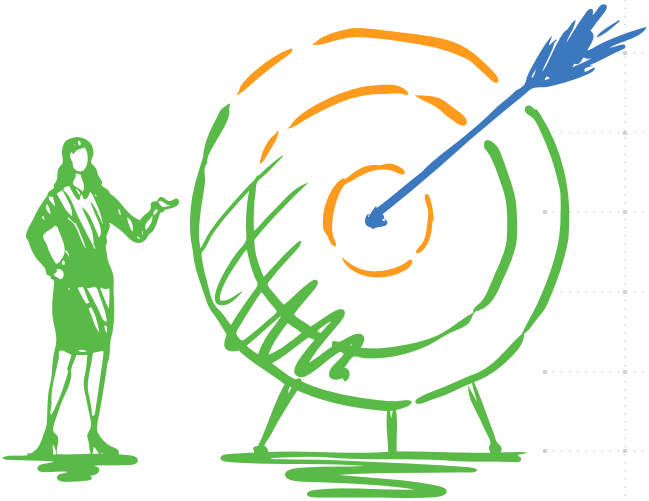
SOURCES

1. Gartner, Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025, July 2025
2. CISA, Zero Trust Maturity Model, April 2023
3. Zscaler, ThreatLabz 2024 Encrypted Attacks Report, December 2024
4. Verizon, 2025 Data Breach Investigations Report, April 2025
5. Google, HTTPS Encryption on the Web, 2025
6. Trend Micro, AI is Accelerating Cyber Risk Exposure, April 2025
7. CyberArk, 2025 Identity Security Landscape, June 2024
8. Verizon, 2025 Data Breach Investigations Report, April 2025
9. IBM, Cost of a Data Breach Report 2025, August 2025
10. IBM/Palo Alto Networks, Capturing the Cybersecurity Dividend, January 2025
11. Sophos, The Human Cost of Vigilance: Addressing Cybersecurity Burnout in 2025, September 2025

ABOUT

exactmarket™

A WBENC-CERTIFIED WOMAN-OWNED BUSINESS ENTERPRISE



Founded in 2007, Exact Market is a woman-owned, WBENC-certified business focused on unifying marketing and technology around a shared vision to help enterprises innovate with confidence.

We bring together strategy, creativity, and data to help our clients stand out and stand for something. Our team of strategists, writers, designers, and technologists understands that the future of storytelling and software shares the same foundation: clarity, authenticity, and human connection.

We don't just help you talk about innovation.

WE HELP YOU LIVE IT.

Find out more: www.exactmarket.com

exactmarket℠

ELEPHANT IN THE ROOM EBOOK SERIES