risk exposure accordingly. Policies can also be enforced when unmanaged devices access sanctioned SaaS applications. This helps prevent exfiltration of sensitive data across all cloud applications.

- **API deployment** provides deeper protections for sanctioned, enterprise-approved applications and performs several functions, including data leak prevention for all data at rest in the cloud application or service, as well as ongoing monitoring of user activity and administrative configurations.

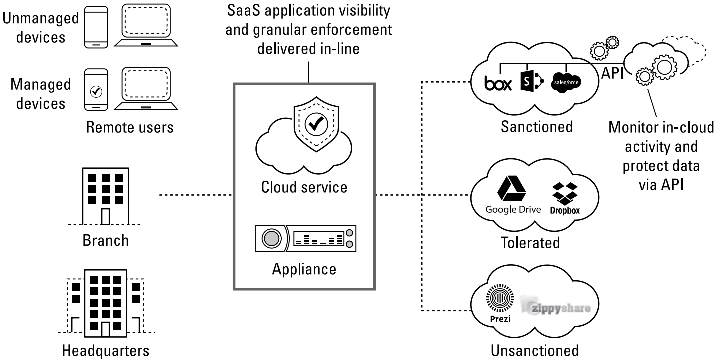


FIGURE 2-3: SaaS security approaches.

In the same way, IaaS and PaaS cloud components must be secured, SaaS applications, such as Box, Dropbox, GitHub, Google Drive, Office 365, and Salesforce, must also be protected using consistent policy enforcement, regardless of application and cloud provider.

Multi-cloud security requirements

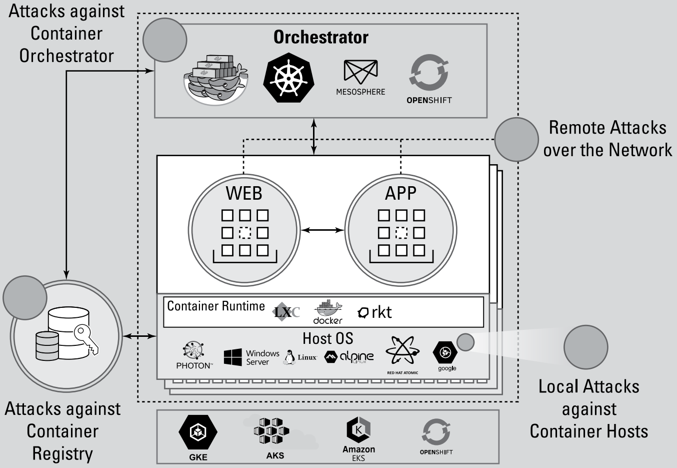
Enterprise data and applications now frequently reside in a multitude of cloud environments, including private and public clouds, spanning IaaS, PaaS, and SaaS.

Despite this momentum, several barriers still slow adoption, and security remains a top concern. Also, although native public cloud security controls provide some degree of access control and identity management, breaches are often the result of improper use, misconfigurations, or advanced threats. Confidently accelerating the move to the cloud requires consistent, automated protections across multi-cloud deployments that prevent data loss and business downtime.

MICROSERVICES ARCHITECTURE AND CONTAINER SECURITY

Microservices architectures (discussed in Chapter 1) and container technologies, such as Docker, Kubernetes, Mesosphere, and OpenShift, are enabling new application architectures for legacy apps, refactored apps, and microservices, among others. Containers are popular among DevOps teams, in particular, because they provide a fast and relatively easy way to quickly deploy new application workloads in a self-contained “infrastructure as code” package that enables standardization, portability, efficiency, and scalability.

However, these new application architectures also introduce new attack vectors including control plane attacks against the orchestrator, network-based attacks across the infrastructure, container registry attacks, and host operating system attacks (see the figure).



Current approaches toward securing container infrastruture are insufficient. These include built-in container security that is immature and ineffective, container security point products that have limited scope and do not address the security needs of hybrid applications that use containers and virtual machines, and legacy network security tools that negate the value of containers.

To properly secure container environments, organizations need to deploy in-line network protections and host operating system security and API-based continuous monitoring and compliance checks. These security tools enable breach prevention, registry scanning, and orchestrator protections for information assurance, assessment, and monitoring.

As organizations embrace multi-cloud architectures, many will continue to support on-premises applications within traditional data centers or private clouds. Protecting these data centers, as well as your multi-cloud environments, requires a comprehensive, consistent security strategy. Consistent security becomes even more powerful when you share threat information across the security infrastructure.

Beyond securing your multi-cloud environments, a comprehensive security platform spans the network and endpoints as well. These security mechanisms — in clouds, networks, and endpoints — essentially act as sensor and enforcement points, working together to arm your business with the collective intelligence required to prevent successful cyberattacks.

Best Practices for Deployment

For enterprises that use the cloud, the key to being protected starts with understanding the layers that make up the components of their cloud stack (see Figure 2-4). These different layers — services, identity, app edge, load balancer, compute, and storage — create multiple potential targets, and for the informed, each represents a piece of the cloud environment that can be secured against potential threats.

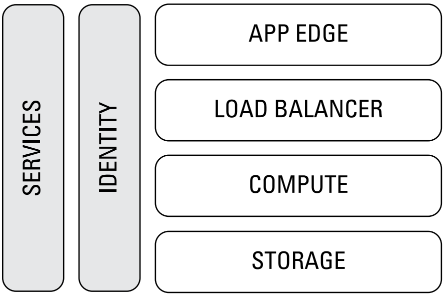


FIGURE 2-4: The layers of the cloud stack.

By focusing on the different pieces of the cloud stack and addressing their unique security threats, your environment will be far more resistant to cybersecurity threats. These best practices will help you secure all layers of your stack:

- **Lock down identity management.** Identity and access management determines what parts of the cloud stack you have access to, and what you can do when you're there. If a bad actor can gain access to your systems using your credentials, you're done. Do the following:
  - **Require secure passwords.** Use the longest password or passphrase allowed by the system, or use a complex password that includes a mix of letters, numbers, and symbols.
  - **Implement MFA everywhere.** Having a strong password is not enough these days. You need multiple layers of protection. Using a second validation or authentication method provides another layer of protection for your user login.
  - **Create least privilege roles.** Only give users access to the least amount of accounts and systems that allow them to be productive. This limits the damage that can be done if a mistake is made or a bad actor gets access to the account.
  - **Disable inactive accounts.** When people leave your organization, disable their access to all systems and disable their access keys immediately. Inactive accounts leave more endpoints vulnerable, and account activity is not usually monitored the same as active ones.
  - **Monitor for suspicious user behavior or compromised credentials.** Use real-time monitoring that leverages machine learning and analytics to identify suspicious activity and possibly compromised account credentials.
- **Secure the compute layer.** Take steps to secure your compute layer to ensure availability of systems and data, and to keep bad actors from using your compute power to further spread malware across your business and the Internet. Do the following:
  - **Harden the operating system.** Remove unnecessary programs that only serve to broaden your attack surface. Stay up to date on service packs and patches as much as

    you can. You may still be vulnerable to a zero-day attack, but it makes such an attack much less likely.

  - **Continuously check for misconfigurations and anomalies.** Use automated tools to detect changes across the environment, as well as anomalous behavior.
  - **Enable secure login.** Issue Secure Shell (SSH) keys to individuals. This will keep your assets protected when moving across unsecured networks.
  - **Implement inbound and outbound firewall rules.** Take care to set definitive rules about what, how much, and who can send, receive, and access both inbound and outbound data. Many organizations are reluctant to set up outbound rules, but because attackers will attempt to steal (exfiltrate) your sensitive data and intellectual property, it's important to ensure you have outbound rules that are explicitly defined. These firewall rules need to be created at the Application layer rather than the Transport or Network layer (IP and port information) to prevent attackers from piggybacking off open ports (such as the domain name system [DNS] on port 53).
  - **Use only trusted images.** Build your images or templates from scratch or get them from very trusted sources like AWS or Microsoft Azure. Don't use images from Stack Overflow or random message boards and user communities.

- **Secure your storage.** If data is the new oil, you want to be sure to protect your precious resources. If attackers get access to your storage layer, they can potentially delete or expose entire buckets or blobs of data. Do the following:
  - **Manage data access.** Identity and access management (IAM) policies and access control lists (ACLs) help you centralize the control of permissions to your storage. Security policies allow you to enable or deny permissions by accounts, users, or based on certain conditions like date, IP address, or whether the request was over a Secure Sockets Layer (SSL) encrypted session.
  - **Classify data.** Automatically classify data to ensure you know what type of data is stored and where it's stored. Data classification policies should be matched to security policies, and any violations should be flagged or automatically remediated.

  - **Encrypt, encrypt, encrypt.** Encrypt your data both in transit and at rest. Note that the metadata is often not encrypted, so be sure not to store sensitive information in your cloud storage metadata.
  - **Enable versioning and logging.** Versioning allows you to preserve, retrieve, and restore data if something goes wrong. With versioning turned on, you can always restore from an older version of the data if a threat or application failure causes loss of data. Maintaining access logs provides an audit trail in case someone or something gets into your system.
  - **Do not allow Delete rights (or require MFA for Delete).** You can set up roles in your cloud infrastructure that do not allow users to delete any data. In many cloud storage solutions, you can also enable a feature that requires MFA to delete any version of data stored in your storage layer.
  - **Continuously check for misconfigurations and anomalies.** Use automated tools to detect misconfigured storage and permissions settings, as well as anomalous file access behavior.

- **Protect your cloud services.** After you've secured the perimeter and enforced smart policies, you need to focus on security specifically for your services in the cloud. Use source control to secure versions, access to builds, and deployment instances. This will reduce the surface area of your code and limit the potential for attacks across your entire network.

IN THIS CHAPTER

- » Exploring how cloud impacts GDPR, NIS, and other regulations
- » Leveraging automation and continuous monitoring to help achieve compliance
- » Getting ahead with a proactive compliance strategy

Chapter 3 Looking at Regulatory Compliance in the Cloud

In this chapter, you learn about select data protection and cybersecurity laws relevant to the cloud, the need for automated, continuous compliance monitoring, and how to be proactive in your compliance efforts.

Navigating the Regulatory Landscape

The regulatory landscape is constantly evolving, with an ever-increasing number of laws and statutes worldwide mandating information security and data protection requirements. Along with more established regulations and standards, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA), U.S. Gramm–Leach–Bliley Act (GLBA), SWIFT data protection policies, Payment Card Industry Data Security Standard (PCI-DSS), and Canada Personal Information Protection and Electronic Documents Act (PIPEDA), recent laws and regulations have garnered much attention, including the European Union's (EU) General Data Protection Regulation (GDPR) and Network and Information Security (NIS) Directive (EU 2016/1148), both of which became enforceable in 2018. These new laws, among others, have important implications for organizations operating in the cloud.

REMEMBER

Compliance requirements are typically based on information security best practices, but it’s important to remember that security and compliance aren’t the same thing.

The GDPR applies to entities that control or process personal data on individuals located in the EU. Personal data is defined in the law quite broadly as any information relating to an individual that is identified or identifiable. In general, this happens in one of the following scenarios:

- The data identifies or can be used to contact a person (for example, name, email address, date of birth, user ID).
- The data identifies a unique device (potentially) used by a single person (for example, an IP address or unique device ID).
- The data reflects or represents a person’s behavior or activity (for example, location, applications downloaded, websites visited, and so on).

The GDPR represents a fundamental shift for personal data protection in the EU. It is much stricter than previous data protection laws, with greater scope of coverage — including companies outside the EU — as well as new data breach notification requirements and significant administrative fines.

The GDPR also introduces mandatory notification requirements for breaches of personal data. Supervisory authorities must be informed, in most instances, if personal data is lost, stolen or otherwise compromised without undue delay and, where feasible, not later than 72 hours after having become aware of it. In certain cases, individuals must be notified as well. Notifications must describe a range of details about the breach, such as its nature, categories, and number of personal data records concerned, likely consequences, and measures taken to address the breach and mitigate its effects.

The GDPR also stipulates administrative fines. The consequences of noncompliance (whether egregious or accidental) can be severe: a potential maximum fine of 4 percent of annual global revenue (or maximum €20,000,000, whichever is higher) for noncompliance with its data processing and data management obligations (such as the requirement to get consent, or various rules regarding data transfers to third countries), and 2 percent (or maximum €10,000,000, whichever is higher) for security and data breach notification-related obligations, amongst others.

WARNING

The potential reputational harm of data breaches, in addition to the GDPR's mandatory notification mandate, the possibility of regulators' investigations, and significant administrative fines, has firmly placed personal data protection as a board-level concern.

TIP

The GDPR is likely to require substantial technology, personnel investments, and business process changes for companies to achieve compliance. The GDPR will impact different groups within an organization, including the legal department, the privacy office, and the chief information security officer (CISO), as well as business teams and product engineers that must implement "privacy by design."

REMEMBER

Privacy by design means that within the architecture of the application, network, or transport, the organization has taken measures to ensure the privacy of personal data, regardless of the type. To this end, the organization must understand the risks of collecting this information and build their systems with the appropriate security. This represents a shift in thinking for many organizations because they now must integrate security into their design process for architectures that are dealing with any kind of accounts or data. "Privacy by default" is a sister concept to privacy by design in that it accounts for the information that is collected, and how organizations must strive to collect the minimum information necessary and minimize their handling of this data.

The vast majority of GDPR requirements center around data management, namely data collecting and processing. There are obligations to provide notice when collecting personal data, prohibitions of unauthorized data processing, requirements to maintain records of data processing activities, a duty to appoint a data protection officer (DPO) in certain instances, and rules regarding transfer of personal data to third parties and third countries, amongst others.

But this should not overshadow the fact that data security is also a pillar of GDPR. GDPR has specific security-related language, as described in Table 3-1. Plus, a key component of protecting personal data is keeping it secure — both from exfiltration by cyber adversaries and from internal leakage. So, as organizations work toward GDPR compliance, it's imperative that investments in compliance activities and information management processes and technologies be complemented with appropriate investments in cybersecurity.

TABLE 3-1 Summary of Relevant Provisions from the GDPR

Topic	Summary of Provisions
Security of data processing	Organizations must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. Those measures must account for the state of the art. **[Article 32]** Personal data should be processed in a manner that ensures appropriate security and confidentiality of the data, including for preventing unauthorized access to or use of personal data and the equipment used for the processing. **[Recital, paragraph 39]** In assessing data security risk, consideration should be given to risks presented by personal data processing. Risks that should be considered include accidental or unlawful destruction, loss, alteration, and unauthorized disclosure of, or access to, personal data. **[Recital, paragraph 83]**
Data breach notification	Supervisory authorities must be notified if personal data is lost, stolen, or otherwise compromised, unless the breach is unlikely to result in a relevant risk to the individual. Notification must happen without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. In certain cases, individuals must be notified. Notifications must describe a range of information about the breach, such as its nature, categories and number of personal data records concerned, likely consequences, measures taken to address the breach and mitigate its effects, and other items. **[Articles 33 and 34]**
Administrative fines	Supervisory authorities are to impose administrative fines for GDPR infringements, on a case-by-case basis. When deciding whether to impose a fine and the amount, the authorities are directed to consider many factors, including the degree of responsibility in implementing technical and organizational measures, taking into account the state of the art as per Article 32. **[Article 83]**

TIP

The GDPR calls for technical and organizational security measures that account for the state of the art. Legacy security systems, made up of cobbled-together point products, have proven inadequate to prevent the rising volume, automation, and sophistication of cyberattacks. CISOs should review these legacy products carefully to determine whether they meet the state-of-the-art requirement of the GDPR.

The Network Information and Security (NIS) Directive is the EU's first law specifically focused on cybersecurity. Its goal is to improve the cybersecurity capabilities of the EU critical infrastructure by establishing security and incident notification obligations for various organizations that offer essential and digital services. The NIS Directive also requires member states to enact national cybersecurity strategies and engage in EU cross-border cooperation, among other measures.

Not to be confused with a regulation, the NIS Directive sets out objectives and policies to be attained through legislation at an EU member state level within a certain time frame (a process called *transposition*). Member states were required to transpose the NIS Directive into national law by May 9, 2018.

The NIS Directive requires that Operators of Essential Services (OES) and Digital Service Providers (DSP) use the state-of-the-art technologies to manage risks posed to the security of networks and information systems used to provide the covered services. These entities must also take appropriate measures to prevent and minimize the impact of incidents affecting the security of the networks and information systems that are used to provision essential or digital services, to ensure the continuity of those services. Security incidents of certain magnitude must also be reported to the appropriate national authorities. These obligations apply whether the OES or DSP manages its own network and information systems, or outsources them to the public cloud (for example).

Recognizing the Importance of Automated, Continuous Monitoring

Security and compliance are shared responsibilities in the public cloud. Many organizations make the mistake of believing that because a public cloud provider manages the security and compliance *of* the cloud, it is also responsible for security and compliance *in* the cloud. That's not the case. It's your data at the end of the day, and if there is a breach or compliance violation, your company will be accountable. The cloud provider delivers a service; the security of your workloads and data is your responsibility as a consumer of the service. It's your revenue, reputation, and customer relationships that are at stake.

A cloud security model should focus on continuous monitoring for, and management of, cloud security risks and threats. Leveraging modern tools and automation techniques to ensure that the organization is aware of and prepared to address vulnerabilities at all times is absolutely essential in the modern threat landscape. This demands the ability to rapidly discover and identify threats in real time; understand their severity; and then immediately act through automated policies, processes, and controls. Point-in-time snapshots of the environment are no longer adequate to ensure protection in the face of dynamic, constantly evolving automated threats.

Organizations must measure security and compliance results constantly, with robust reporting capabilities in the event of an external audit, for example. Achieving this state of continuous security-first compliance requires the use of modern tools and a security platform that leverages the application programming interface (API)–centric architecture of the public cloud.

By using a platform that enables continuous monitoring and management of security in the cloud against policy, IT and security teams will have greater assurance that the organization will be compliant within the required frameworks. Benefits of this model include

- Compiling a complete unified view across all cloud services
- Generating compliance reports without the need for specialized knowledge
- Identifying, prioritizing, and remediating compliance risks as they arise with automation driven by machine learning and analytics — without requiring human interaction
- Monitoring compliance throughout the entire development life cycle
- Avoiding "last-minute fire drills" to meet compliance requirements
- Demonstrating to auditors that the organization is managing security 24/7/365 — not just in the last few weeks before an audit

Compliance and application development teams can both benefit from continuous monitoring and compliance automation. Compliance can significantly reduce time spent on third-party security audits. Application development teams won't get bogged down by compliance audits that stop development projects, thus enabling speed of innovation and development to be competitive differentiators.

TIP

With the right cloud security platform, you can leverage automation to reduce risk and remove the human element from vital processes. This automation allows you to achieve complete and continuous visibility across your cloud deployments, enabling standardized, consistent deployments among usage environments such as development, staging, and production.

Avoiding the "Compliance Catch-Up" Trap

For many organizations, compliance is a never-ending cycle of audits, reactionary efforts to correct audit discrepancies, and an inevitable drift from the compliant state over time. This "no-win" situation frustrates everyone in the organization and can derail other projects and security initiatives. The speed of deployments and the pace of change in the cloud creates an impossible situation and, frankly, a futile effort for organizations that rely on legacy tools and manual processes to secure their cloud environments and achieve compliance.

Fortunately, new cloud security tools are now available, delivering an agentless platform designed specifically for public clouds and SaaS environments. These solutions leverage the cloud's API to derive tremendous flexibility in scaling and managing cloud security and compliance.

The following steps describe how a modern automated approach to continuous cloud security and compliance works:

- **Step 1: Monitoring.** The cloud environment is changing continuously. These changes can be normal, routine activities of your DevOps or IT teams; they can also be the work of people who would do harm to your business. As changes are made — across all clouds, regions, and services — the cloud security platform monitors the configurations of the infrastructure to ensure that it adheres to security and compliance best practices.

- **Step 2: Evaluation.** The security platform securely collects data about your cloud services and continuously performs checks against a series of predetermined security best practices and compliance guidelines. It also performs checks against any predefined custom signatures. These checks determine, on a continuous basis, whether there are any potentially exploitable vulnerabilities.
- **Step 3: Deep analysis.** The platform performs an analysis to determine whether the discovered misconfigurations and exposures are ranked as high, medium, or low risk.
- **Step 4: Automated remediation.** The resulting analysis is displayed on a dashboard and predetermined items can be sent to integrated systems for auto-remediation workflows to kick in, when possible and appropriate.
- **Step 5: Robust reporting.** Detailed reports are made available, so your teams can see information about the risk, including user attribution and affected resources. Audit reports from reporting and tracking are also available for compliance efforts.

FOUR WAYS TO IMPROVE CLOUD SECURITY AND COMPLIANCE

The cloud requires a new way of approaching security. Traditional data center and endpoint security technologies and methodologies are not adequate to protect the highly connected architecture of the cloud. Without a modern, cloud-first approach, security will be compromised because of a variety of factors.

The inherent risk-related challenges can be addressed by employing a security platform built for the cloud that leverages automation to provide continuous monitoring, analysis, prevention, and remediation for cloud security and achieving compliance.

This is a new model that provides comprehensive protection in the cloud. As organizations continue to rely on public cloud to drive day-to-day business activities, as well as innovation, they must reduce security risks and simplify the processes involved in ensuring protection and compliance. Continuous security and compliance present a new opportunity to maximize the value of the public cloud while minimizing risk.

Security experts seek innovative, but usable solutions, and say it is important to focus on four key elements to achieve continuous and automated cloud security and compliance, as follows:

- **Rapid discovery to keep up with the fast pace of change in the cloud:** With the enormity of deployments in the cloud, it isn't unusual for organizations to have millions of data points (such as user or application behavior and configuration settings for cloud services) that need to be evaluated. You need a platform that can handle all the data in real time and rapidly isolate any security variation or deviation from known states.
- **A "single pane of glass" to view your entire cloud environment:** When teams are very large, communication can falter. With each team using different tools to gain a different view of the environment, information becomes siloed and difficult for other teams to understand. Your platform should let teams own their own security, while also providing a "big picture" view to security operations teams and corporate management. The platform must be able to evaluate security data in isolation, as part of the global customer base or across time and geography, to warn about potential issues before they occur.
- **Automated response:** Organizations need to automate not only monitoring and analysis, but also remediation to fix permission or configuration errors. They should have flexibility in determining the course of automated response, with the ability to inform human administrators if there is any other action that may be required.
- **Robust reporting:** Teams need to be able to measure and demonstrate security and compliance progress daily, not just during the yearly audit. With the right platform, you can show your security and compliance posture at the push of a button.

IN THIS CHAPTER

- **Identifying the cybersecurity resources and skills your organization needs**
- **Aligning cloud maturity and automation levels**
- **Creating a secure application development culture**

Chapter 4 Building an Organizational Culture around Security

In this chapter, you explore the key elements of creating an effective cybersecurity team, how to leverage automation to augment your cybersecurity team, and how to build a secure application development culture within your organization.

Creating an Effective Cybersecurity Team

Enterprise security isn't easy — and the speed at which enterprises are moving today to innovate and deliver digital services isn't making the challenge any more straightforward. Considering aggressive timetables and delivery deadlines, it's easy to let the discipline required for security slip. But with today's hyper-connected world, and fast-moving and changing cloud environments, letting security slip for even a moment is just something that enterprises simply can't afford. To succeed, enterprises must have the processes and technology — and most certainly the people — in place to keep systems adequately secured.

Creating an effective cybersecurity team begins with an assessment of your organizational needs. This includes identifying teams that may need to be created within the organization (for example, incident response and compliance audit teams), as well as the required skill sets. Next, identify any skills gaps that exist within your current cybersecurity team and determine whether those skills can be attained with training for current team members or whether additional team members need to be hired.

When assessing your organization's cybersecurity needs, remember that automation can enable more rapid response to security incidents by eliminating manual security tasks. Automation thus frees up existing team members to perform other value-added cybersecurity tasks while also limiting the need to hire additional team members. Automation can be a bridge between the shortage of qualified cyber talent in the market and effective cybersecurity.

A recent joint research project by the Enterprise Strategy Group (ESG) and Information Systems Security Association (ISSA) found that 28 percent of cybersecurity professionals and ISSA members feel their organizations depend upon too many manual processes for their day-to-day security operations, such as chasing down data, investigating false positive alerts, or managing remediation tasks. This is exacerbated by a looming shortage of skilled cybersecurity professionals.

There simply aren't enough hours in the day to get to everything, no matter the skill level of your cybersecurity team. With automation, advanced analytics, and security integration, you can begin to bridge the gap. From the cyber defender's perspective, there are three ways to think about automation:

- **Turn threat detection into prevention.** Organizations shouldn't spend any time manually preventing known threats, because prevention should be automatic. The same goes for unknown threats — they need to be automatically analyzed and blocked if they're malicious.
- **Adapt to dynamic environments through context-based access policies.** The IT landscape is constantly changing. Security teams must be able to set policies based on the context of what should be protected: users, data, and applications. Context-based policies stand the test of time and adapt to business changes without requiring constant updates.

- **Automate investigations using analytics and machine learning.** Automation supplies critical leverage, giving organizations an edge over adversaries with insight and context around exploits and techniques. With next-generation firewalls that can ingest third-party data feeds and dynamically update policies, automation turns information into prevention. By using rich security data across locations and deployment types, analytics and machine learning find hidden threats and reconstruct attacks. Both of these automation capabilities save you valuable time.

TIP

A security vendor that offers automation essentially gives you back time to do more valuable, business-critical work. It allows your security teams to move away from basic operational tasks and focus on strategic efforts that directly benefit and improve the security and compliance posture of your organization.

Finally, it's important to know what success looks like for the team. Object key performance indicators (KPIs) should be defined to help the team continuously assess its effectiveness in protecting the organization's cloud assets. Some potential KPIs might include

- Number and types of security incidents reported
- SaaS usage, including misconfigurations, accidental sharing, and promiscuous sharing
- Instances of improperly secured virtual private clouds (VPCs) in Amazon Web Services (AWS) and Google Cloud Platform (GCP), and virtual networks (VNets) in Microsoft Azure
- Time to detect security breaches
- Time to remediate breaches and incidents
- Vulnerabilities identified and patched
- Threats prevented

Recognizing How Cloud Maturity Affects Automation Levels

Your organization's cloud maturity (discussed in Chapter 1) largely determines automation levels throughout your environment. Automation can oftentimes be applied to processes throughout the security organization, not just in the cloud. Organizations that already use automation extensively in their cybersecurity processes understand the value of automation in reducing potential configuration errors and enabling rapid security response actions when threats are detected, among others.

For intermediate (cloud implementers) and advanced (cloud optimizers) businesses, automation becomes increasingly important as these organizations increase cloud usage, expand to multicloud deployments, and optimize cloud operations. With automation these organizations can successfully scale their cybersecurity operations and reduce the risk of error, allowing them to protect the organization's entire cloud footprint.

REMEMBER

Automation helps secure the business by

- Creating touchless deployments so that security can be enabled for application development teams and protect the environment from threats without slowing the business
- Flagging non-compliant services as they're spun up and dynamically updating policies as the environment changes or new threat information is collected

Embedding Security in the Developer Workflow

Moving at the speed of the cloud raises the concern that costly mistakes could happen. The worry is that as processes are automated, and rapid decisions are made in an environment that prioritizes agility, security compromises will be made. Different stakeholders (such as application development teams and individual business groups), who may not be focused on the broader security picture, now play a more significant role in the cloud conversation. If not properly addressed, unintended consequences — such as security holes due to misconfiguration, choosing "good enough" security, or forgoing security considerations altogether — may ensue.

Compounding this challenge, enterprises face an unprecedented shortage of professionals with cybersecurity skills, especially skills that are critical when it comes to securing DevOps organizations and cloud environments. Consider how much this gap has grown in recent years: A recent survey conducted by Enterprise Strategy Group found that 45 percent of organizations currently report having a "problematic shortage" of cybersecurity skills.

Cloud computing does help to simplify some areas of security, but it doesn't simplify everything. Enterprises are still responsible for the security of their data, applications, operating system, network, firewall configurations, and so on. And although DevOps helps to speed development, it can be challenging to adapt security techniques to keep pace with new application development and deployment capabilities.

TIP

In its October 2017 "10 Things to Get Right for Successful DevSecOps," Gartner wrote, "Don't force information security's old processes to be adopted by DevOps developers. Instead, plan to integrate continuous security assurance seamlessly into the developer's continuous integration/continuous development (CI/CD) toolchain and processes."

So, how can enterprises provide their teams with everything they need to keep their systems secure? It certainly requires having the right technology and processes in place. But getting them in place and keeping them there requires both assembling the right team and making sure everyone on the team does his or her part. But how are these skills cultivated? And how does security become an integral part of the culture of the organization?

The following critical elements will help an enterprise form a smart framework for running a DevOps organization:

- **Continuous cybersecurity skills training and enhancement:** DevOps teams adhere to security best practices, but how those are implemented, and the speed at which they're used must adapt to the speed and agility of a DevOps environment. What does successful implementation of security essentials look like? It's when the entire DevOps team understands security basics including managing secure access to cloud environments, keeping configurations in a secure state, and putting automated controls in place. How is this achieved? Cross-training and more security training. Train operation teams on good security practices, how to use relevant security tools and how to script securely. The same goes for developers who should be continuously trained on secure coding practices to create security champions within the DevOps team. And, above all, security professionals need to be in continuous contact and collaboration with the rest of the technology teams (for example, development and networking).

REMEMBER

To build a team that can keep systems secure at the speed of DevOps, you need staff that collaborates, understands each other's strengths and weaknesses, helps each other to compensate for those differences, and continuously cross-trains.

- **Security from design through production:** Security efforts should be an integral part of the entire IT process, from the new product, feature, or application design phase through development, application testing, and into production. Too often, security is first addressed during the quality assurance phase or, worse, in production. Staying secure and compliant requires continuous and automated security monitoring of all systems running in production.

  REMEMBER

  To properly manage risks, security must be an integral part of the design, development, and production life cycle.

  TIP

  Integrating security processes and built-in security controls into DevOps empowers application development teams with a DevSecOps model that ensures security is properly addressed throughout the application development life cycle.

- **Executive leadership:** Talk with any CIO or CISO about what it takes to build a security-aware DevOps team and the top answer — nearly unanimously — will be that leadership support is the determining factor. Successfully building a secure DevOps organization requires leadership that will help to drive and instill security culture and processes.
- **Automation:** Through automation, you can accomplish two critical prevention-focused tasks:
  - You can embed security into your application development workflow, ensuring security keeps pace with development.
  - You can ingest external information that can be used to drive/create policies that are dynamically updated as workloads are added or removed from your cloud environment or as new potentially malicious threats are discovered.

  REMEMBER

  When a process can be automated, it should be automated.

- **Cultivating the collaborative mind-set:** The spirit of DevOps is to break down the silos in IT departments among developers, operations teams, IT leadership, quality assurance (QA), and security, and embed security as a priority throughout all aspects of development and management. However, for most enterprises, security has been more of a roadblock than an enabler. Communication among security managers and every other team is essential so that everyone comes to understand the roles and challenges of others on the team and identify opportunities to improve. This has always been how the relationship between security and the rest of the IT and development teams should be, but it's especially true for DevOps. Most important to success here is communication and empathy regarding the needs of others. Finally, to foster security collaboration, the right incentives should be in place, such as having security-related KPIs that span multiple teams.

  TIP

  Create an environment where the security team collaborates with other groups and sets incentives to help keep such collaboration aligned.
- **Security accountability:** If security is to become an integral part of the organization's DevOps culture, the enterprise will need executive leadership that actively shows it cares about security. This way there will be regular, continuous, and comprehensive conversations at all levels of the business regarding aspects of the security program that need to be in place. This is best achieved by having a CISO in place with backing from the board of directors. Engagement helps to create competent security leadership that aligns with DevOps and keeps security efforts synchronized with business needs.

TIP

To get the DevOps team and the entire organization aligned when it comes to mitigating business risks, it's crucial to have someone who leads the security efforts.

IN THIS CHAPTER

- **Bringing artificial intelligence and machine learning to automation**
- **Preparing for the future with a blueprint for risk**

Chapter 5 Forecasting Changes in Cloud Security

In this chapter, you take a glimpse into the future of cloud computing and security.

Looking at the Direction of Cloud Security

As businesses everywhere continue to migrate their critical applications, workloads, and data to the cloud, public cloud providers will continue to rapidly grow their data center footprints around the world. Data, intellectual property, and compute resources — regardless of their location — are targets for attackers. Hackers' goal is to access the network, navigate to their target, and then execute their attack objectives. The public cloud, by the very nature of its growth and visibility, will be a target-rich environment for attackers for the foreseeable future. Attackers understand the shared responsibility model (discussed in Chapter 1) as well as — or better than — most cloud customers. As such, attackers for the most part will continue to follow the path of least resistance, seeking to exploit the weakest link in an organization's cybersecurity chain to gain access to their cloud resources, instead of attempting a direct assault on major public cloud providers such as Amazon, Microsoft, and Google, who themselves invest extensively in cloud security resources.

One trend in cybersecurity that will clearly continue in the future of cloud security is automation. The speed and scale of change makes it impossible for organizations to effectively manage their cybersecurity posture in the cloud with manual tools and processes. Attackers have wholly embraced automation to proliferate malware and brute-force account credentials, among other attack techniques. Cybersecurity teams must respond with automation tools and techniques of their own.

Cloud application architectures will also continue to evolve with practically infinite compute processing resources, increased adoption of containers, new innovations in serverless computing, and more. Extremely large data lakes will also be necessary to handle the deluge of data generated by the Internet of Things (IoT), big and small data analytics, machine learning, and more.

These trends will have security implications themselves, but they'll also impact the technologies used to secure enterprise multicloud and on-premises environments of the future. For example, data collection sensors deployed across clouds, users, sites, regions, devices, and so on, will enable ever greater visibility and continuous monitoring across heterogeneous environments. The data generated by these data collection sensors could be hosted as a common data lake of security and threat events, which security vendors can use to build apps or services to add more value and enhance their customers' security and compliance posture.

As artificial intelligence (AI) and machine learning (ML) technologies continue to mature and advance, automation will become more critical in areas such as threat detection and security analysis, particularly given the deluge of sensor data and threat information. Discrete anomalies will increasingly be detected and stopped in real time, effectively closing the window of opportunity for cybercriminals.

Drafting a Blueprint to Manage Risk

Keep in mind that your move to the cloud means that not only has your risk of breach changed, but you also have increased risk of failure. Developers could take a system down with the click of a button or one wrong line of code in an application deployment. Look to build protections that will reduce security risk and also ensure the availability of critical systems and data. As you rearchitect systems and begin utilizing new technologies and architectures like containers and microservices (or whatever comes next), consider how you'll test to ensure that systems are performing as designed and delivering the expected results.

You need to adapt your existing risk management and cybersecurity frameworks to address the cloud, as well as new and evolving technologies. The NIST Cybersecurity Framework is one example of a great framework to help you get started. The following sections cover the core functions of the framework and how they're affected by your move to the cloud.

Identify

As you prepare for the future, review your current tool set and skill set to ensure that your team is able to take advantage of new advancements in automated monitoring, detection, reporting, and machine learning. Traditional data center solutions are often unable to keep up with the high volume of data and speed of change. Embed automated security scanning into your DevOps workflows, so that analysis and testing become an integrated part of your development life cycle. To speed adoption, don't make developers learn new tools. Instead, look for tools that support application programming interface (API) enablement and provide rich context.

REMEMBER

If data is the new oil, then machine learning is the new filter that makes it usable by your teams and systems. Leveraging algorithms to discover and classify large amounts of data is a must in the cloud.

Protect

It used to be that we only had to protect and defend what was inside the perimeter of our data center and our network. However, as organizations move more workloads to SaaS systems and the cloud, network perimeters are expanding and becoming less distinct at an exponential pace. You now need to protect inside your network, across multiple clouds, and out to wherever your mobile users are connecting to the network. Now that the world is your perimeter, you need different means and tools to protect it. Implementing a Zero Trust security model (discussed in Chapter 6) will help set your organization up for success in the cloud.

Detect

Every organization has been impacted by the shortage in security talent, so it is becoming imperative that organizations of all sizes begin leveraging automation to continuously monitor and analyze events and the effectiveness of deployed controls and protections. Keep in mind that in the cloud, services, virtual machines (VMs), and configurations can change rapidly. In fact, some microservices may exist in your cloud environment for only a few minutes. You must be certain that the tools you employ to detect and log changes can keep pace with these rapid fluctuations.

TIP

Cloud technologies can make certain aspects of the detect function more challenging, but they can also be used to your advantage. Consider using security technologies and services to leverage advanced techniques to detect issues, whether vulnerabilities or attacks, in your networks and systems. Technologies and tools that make use of machine learning to address well-defined security problems, like classifying data for compliance purposes, analyzing and correlating events in log files to find insider threats, or identifying malware and advanced threats across all your endpoints, are just a few examples.

Respond

When things go wrong, recognize that you need to do more than just stop an attack. You need to know what was impacted, understand what data was accessed, recognize whether there is a compliance impact, and know what your responsibilities are to report the incident.

Today, this function is as much a business response as it is a technical response. Business leaders need to work closely with security and IT teams to ensure that projects are executed within an acceptable level of risk. Response plans need to rise to the level of the board and executive management to ensure they're prepared in the event a major incident impacts the business. Lessons from the Equifax breach or the impact of the Yahoo! breaches on its sale to Verizon are not-so-subtle reminders of how important security and public relations are to the valuation and long-term viability of a business.

As part of your response plan, you can use advanced technologies, such as security tools that streamline the orchestration of threat intelligence and enforcement of prevention-based controls. New tools can remove the manual work of intelligence gathering by allowing you to make use of public, private, and commercial intelligence sources across both government and commercial organizations — and also allow you to share your threat indicators with trusted peers to contribute to global cyber defense efforts. These technologies unify your operational, security, and risk management teams through a single source of truth — the same contextual security data from your modern, advanced systems.

Recover

For your recovery efforts, it's important to ensure that you have enough information to know what went wrong, so you can fix it — but in cloud environments the amount of data is enormous. Look for tools that will provide you with a single pane of glass for all your event and security logs and will normalize disparate data types so your operational teams can establish a new security baseline. This new security baseline is used to re-evaluate your existing risk framework and suggest possible improvements.

IN THIS CHAPTER

- » Adopting a cloud-centric approach and knowing your responsibilities
- » Applying "never trust, always verify" to the cloud
- » Engaging stakeholders early
- » Understanding your potential exposure and adversaries
- » Evaluating your options and recognizing the power of knowledge
- » Preventing known and unknown threats in IaaS and PaaS environments
- » Leveraging automation

Chapter 6 Ten (Or So) Cloud Security Recommendations

In this chapter, I outline some key recommendations to protect data and applications in the cloud.

Take a Cloud-Centric Approach

The cloud enables your organization to address business challenges with an agile, more scalable approach. To take full advantage of the cloud, recommended best practices include applying the concepts of the modern data center to your cloud deployment architecture, while leaving the traditional constructs behind. In this way, business-critical infrastructure best practices like high availability and scalability can be achieved organically.

Embrace the Shared Security Model

Public cloud providers, such as Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure, make it clear that security is a shared responsibility. In this model, the provider is responsible for ensuring the platform is always on, available, and up to date.

In fact, the cloud provider's global data center infrastructure is more secure than most organizations' own data centers. However, you, the customer, are responsible for protecting your own applications and data running within the public cloud.

Figure 6-1 highlights the responsibility breakdown. You're in complete control of what security to implement and must take steps to safeguard your content, be that customer data or intellectual property. The benefit of embracing the shared security model is that your team is focused on protecting your apps and data, typically your most valuable assets.

Public Cloud Security Responsibility

Security is on you	Applications (including operating system) and associated data deployed
	Account controls (access control, services enabled, and so on)
	Deployment architecture, configuration management, and so on
Security is on the provider	Worldwide footprint (regional presence and so on)
	Physical components (buildings, server hardware, resiliency, and so on)
	Compute infrastructure (network, database, storage, and so on)

FIGURE 6-1: Public cloud shared responsibility model.

Use a Zero Trust Strategy

What happens when you ink a deal with a public cloud or web service is what is known as the "uneven handshake." The vendor agrees to provide you with an array of services, but it doesn't assume responsibility for managing your cyber risk. Instead, the vendor provides you with a number of options for how you might set up and configure its security tools.

Traditional, perimeter-centric security strategies fail to provide adequate visibility, control, and protection of user and application traffic. Zero Trust architectures apply the principle of "never trust, always verify" to all entities — users, devices, applications, and packets — regardless of what they are *or* their location relative to the bounds of the corporate network (see Figure 6-2).

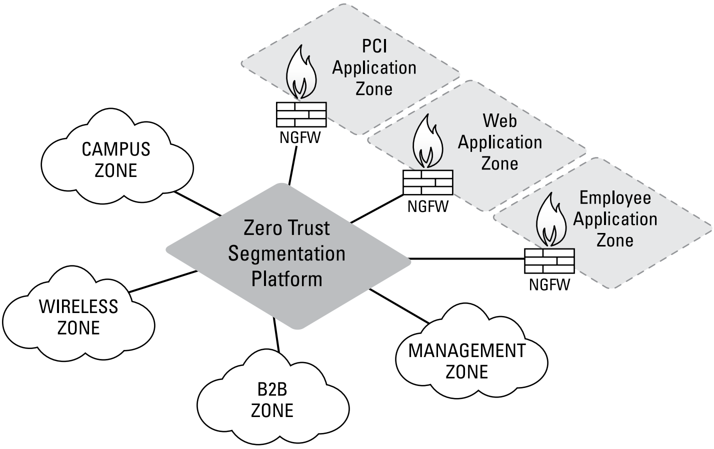


FIGURE 6-2: Zero Trust segmentation platform.

When enterprise leaders are thinking about entering into a cloud agreement, it's critical that they start thinking about a security model for protecting the digital business. What's more, because most companies are in multiple cloud environments, they must be able to put in place and oversee a strategy that encompasses multiple platforms in multiple locations, where regulations can vary dramatically.

By establishing Zero Trust boundaries—just as they would to effectively compartmentalize different segments of their own networks—companies can better protect critical data hosted in the cloud from unauthorized applications or users, reduce the exposure of vulnerable systems, and prevent the movement of malware throughout their network.

Engage with Business Groups, Governance, and DevOps Early

Most cloud projects are driven by business groups and managed by DevOps teams. Quickly spinning up new products or functional prototypes is commonplace and can happen with only a few hours of notice. A common challenge is that the security team is often brought in to review the architecture after the workload is already running in the cloud. By including security and governance earlier in the process, business and architecture decisions will be made with a security-first approach. This greatly reduces the burden of maintaining a secure environment and achieving compliance when required.

Know Your Potential Exposure

Public cloud usage is prolific due to the ease of spinning up compute and storage resources. Employees doing what is "right for the business right now" versus what is "right for the business" may create security holes if the environment is not configured properly. It's imperative to know who in your organization is using the cloud and to ensure the environment is configured correctly. To reduce cloud risk, you should do the following:

- **Monitor cloud usage.** Perhaps the quickest way to determine usage is to look at how much your organization is spending in AWS, GCP, and/or Microsoft Azure.
- **Ensure proper configuration.** Configure the environment with security best practices in mind. Establish secure defaults

for identity and resource access, enable all audit and security logging capabilities, and properly segment workloads into dedicated environments. This gives you a secure baseline from which to implement workload-specific configurations.

- **Require multi-factor authentication (MFA).** To minimize the risk of an attacker gaining access using stolen credentials, MFA should be required. Using intelligent challenge-response mechanisms can also protect apps in the cloud from unauthorized access.
- **Lock down administrative interfaces.** For example, Secure Shell (SSH) on port 22 is a preferred method to securely manage cloud servers, yet it's often left exposed in AWS, GCP, and Microsoft Azure environments for convenience. Other administrative ports, including those for container management systems, application admin consoles, and other similar interfaces should be strictly controlled and protected.

Understand the Attacker

Attackers leverage automation to find potential targets within minutes. When they've identified those targets, they look for weaknesses, checking default passwords, probing for SSH misconfigurations, and so on.

To highlight the effects of attackers' automation capabilities, Palo Alto Networks spun up a test environment with a database and a web server in the public cloud to demonstrate the extent of attackers' capabilities. The environment was probed from more than 35 countries with more than 25 different attacker applications. In Palo Alto Networks' research efforts, a full global scan of all AWS, Azure, and Google Cloud servers took 23 minutes to complete and revealed tens of thousands of exposed systems. Unlike in a private data center, where there is less concern about public exposure, resources in the public cloud are widely exposed and should be handled carefully.

Evaluate Your Security and Compliance Options

There are several security options to choose from when moving to the cloud, most of which are like the options for physical networks, including the following:

- **Native security services:** Cloud service providers offer native security services including security groups, web application firewalls (WAFs), configuration monitoring, and many more. These tools are a good starting point for those without added security technologies, but the capabilities should be supplemented with enterprise-grade security offerings. The following two examples highlight the need for third-party security tools:
  - **Security groups** and port-based firewalls are essentially port-based access control lists, providing filtering capabilities. They cannot identify applications by content, and you won't be able to prevent threats or, more important, stop outbound data exfiltration like a next-generation firewall can.
  - **WAFs** are limited because they can only protect HTTP and HTTPS applications. This means that WAFs can't protect applications that may use a wide range of ports to function properly. Plus, they aren't an effective means of identifying and controlling remote management or access tools, such as SSH or Microsoft Remote Desktop Protocol (RDP).
- **Point products:** Organizations that deploy point products that are designed to solve a particular use case end up deploying numerous products from different security vendors. This creates complexity with a fragmented set of security tools that don't seamlessly integrate and communicate with each other, and require specialized skills to operate and manage. Automation becomes difficult, if not impossible to achieve.
- **Do-it-yourself (DIY) security:** Some organizations choose a DIY approach to securing cloud workloads, using custom scripts and open-source projects to protect deployments. Disadvantages to this strategy include the burden of improving custom tools, lack of expertise to manage the

security implementation and operations, and nonexistent support in the event of a security breach.

WARNING

Organizations that rely on internal personnel to manage cloud and security deployments must be prepared for attrition. Typically, only a few engineers know the environment well, but they don't necessarily have time to keep proper documentation or manage knowledge-sharing requirements. If even one of those engineers leaves the company, the organization may not be well positioned to effectively manage security — particularly DIY security — needs moving forward.

- **Security platforms:** The goal for many organizations is to eliminate a fragmented security approach where the security tools don't communicate with each other to successfully prevent attacks. To overcome this challenge, organizations typically adopt a security strategy that utilizes a platform approach. This approach delivers security through in-line, application programming interface (API)–based and host-based protection technologies working together to minimize attack opportunities:
  - Secure in-line traffic provides inbound and outbound protections, segmentation of workloads, and threat prevention capabilities.
  - Monitor and protect public cloud resources via cloud provider APIs. These resources need to be monitored continuously rather than through point-in-time checks.
  - Maintain the integrity of the operating system and applications on the virtual workloads blocking exploits, ransomware, malware, and fileless attacks.

Empower Yourself with Knowledge

Personal branding consultant John Antonios once said, "Knowledge plus action is power." In cloud security, knowledge begins with ingesting large sets of data produced by the cloud, network, and endpoints. This data then needs to be analyzed to find the threats that need to be acted on to protect your cloud.

Security tools need to be able to share this threat information with other parts of the cloud, points of enforcement, and the broader enterprise-wide IT deployment. Then, to help fight large-scale attacks and ensure future detection of similar attacks, this information needs to be shared with the broader community and security industry.

Attackers must then develop new tools, acquire new infrastructure, or develop different attack techniques from the ones already exposed. These changes require time, money, and other resources, which increase the cost to conduct the attack.

As you build your cloud security strategy for your environment, ensure that your security tools are capable of sharing threat intelligence across your broader enterprise and receiving threat data from external sources.

TIP

To fast-track secure cloud adoption, consult cloud security experts through communities or vendors. The guidance will ensure you build the right security foundation to enable your business in the cloud.

Believe in Prevention

There are those who believe the attackers have already "won," and thus choose to focus primarily on a detection and remediation approach. However, a prevention philosophy is critical to dealing with the volume of threats. Strong prevention minimizes the number of events that require detection and response, allowing you to rapidly stop sophisticated attacks before they can steal confidential data. Enabling the prevention of successful cyberattacks in the cloud requires four key capabilities:

- **Complete visibility:** The combination of knowledge and enforcement is a powerful security tool. It's critical to identify all your cloud resources, ongoing cloud activity, relative risk tied to current security measures, and any changes to your environment. With this knowledge, a more consistent security policy can be deployed globally to protect your cloud from known and unknown attacks.