DEFENSE IN DEPTH

Leveraging the cloud to reinforce 7 critical layers of security

Hyland®

CONTENTS

(click to jump to a chapter)

Is the future of your business safe?

You're in business to *do* good business. To deliver on promises, to help your customers, to foster a place for talented and happy employees — and of course, to thrive.

But if your data and your customers' data is vulnerable to incursions or catastrophic events, the future of your business isn't safe. Without proper defensive measures, your data is unprotected and your ability to service customers can be impacted.

In this ebook, we'll help you:

- Analyze your own defense preparedness
- Discover best practices for staying secure in an environment of ever-changing threats
- Identify opportunities for leveraging the cloud to maximize your levels of defense

Although the world can be full of threats, there is hope: You. Your team. Your willingness to tackle defense in depth.

The ability for an enterprise to outsmart and out-prepare against threats is the first step toward fortifying your future.

Get started on your defense.

What is defense in depth?

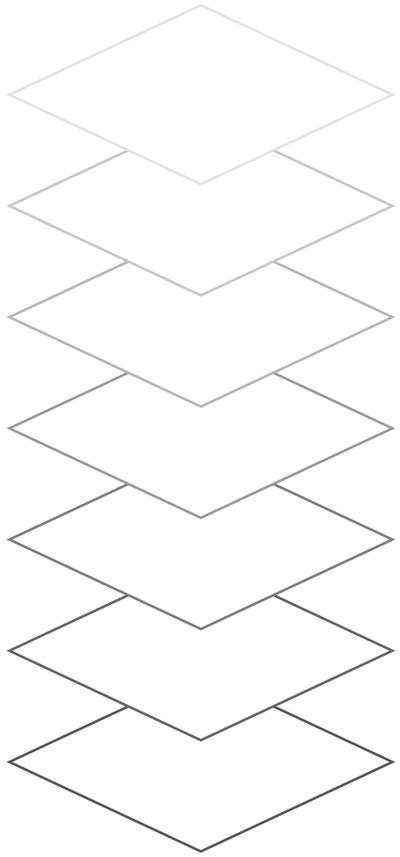
DEFENSE IN DEPTH COMES DOWN TO DIVERSIFICATION OF DEFENSE STRATEGIES

Like a diversified retirement savings plan that spreads investment across different assets, an effective defense-in-depth strategy spreads defense mechanisms across seven layers, so that even if one layer fails, there are six others offering a strong — but different — defense.

The seven independent layers are deployed like concentric circles around your prized core data, increasingly strong and uniquely designed to defend against different threats. Breaching one layer won't give the threat an advantage on the other six layers.

Today, as organizations increasingly look to the cloud as part of their future-proofing plans to support growth and improve customer experience, cloud strategy must also be evaluated in the context of your organization's defense-in-depth strategy:

How does the cloud fit into your defense strategy?



LAYERS OF DEFENSE

1. POLICIES, PROCEDURES AND AWARENESS
2. PHYSICAL SECURITY
3. PERIMETER DEFENSE
4. INTERNAL NETWORK SECURITY
5. HOST SECURITY
6. APPLICATION SECURITY
7. DATA SECURITY

Together, the layers are supplemented by cloud defense mechanisms to provide a diversified response to the infinite variations of challenges that organizations face, such as:

- Malicious acts by hackers or rogue actors
- Technology failures
- Catastrophic events
- Well-intentioned but careless users

HOW IMPORTANT IS YOUR DEFENSE?

How would your business respond to a breach ... that happened five minutes from now?

Here's what impact statistics tell us:

- **$8.64 million:** Average cost of a data breach in the U.S. (the most expensive in the world)[i]
- **$440 per hour:** average incident response cost in the U.S.[i]
- **280 days:** Average time to identify and contain a data breach[i]
- **$1 million:** Average savings from containing a breach in under 200 days, compared at over 200 days[i]
- **$141:** average global cost per impacted data record[ii]
- The European Union's General Data Protection Regulation (GDPR) violations[iii]
  - Infringements: €10 million or 2 percent of a firm's worldwide annual revenue
  - Severe infringements: €20 million or 4 percent of a firm's worldwide annual revenue

layer 1:

POLICIES, PROCEDURES AND AWARENESS

Every business depends on its people, and oftentimes we hear, “Our people are our greatest asset.”

We agree.

But, with great power comes great responsibility. Today, your employees have access to staggering amounts of sensitive information. Oftentimes, your partners and vendors have access to your data as well. As your organization must now comply with a growing number of regulations and requirements for how this data should be stored and accessed, you must create a culture that promotes adherence to policies, implementation of standardized data processes and continued security and compliance education. Your employees’ and partners’ knowledge about the importance of keeping your data safe — and their behavior in doing so — is the first line of defense against data breaches.

THE TAKEAWAY: People can be your weakest link — within your organization or beyond it. Get everyone on board with a culture of strict data security.

Fortify your people and your culture »

WHAT GOOD DEFENSE POLICY, PROCEDURES AND AWARENESS LOOKS LIKE

Strong password security and Single Sign On (SSO)

Password strength and security is critically important. Employees and contractors need to know and embrace that passwords should be long and complex, never written down or shared, and applied to any device used for business and unique to the account.

What it protects you from

- Malicious actors looking for easy entry points
- Applications with weak password requirements

Multifactor Authentication (MFA)

MFA helps ensure the person accessing your network and data are who you think they are. It requires users to present two or more pieces of evidence to get access to a system and can range from passcodes to biometric traits.

What it protects you from

- Lost or stolen devices falling into the wrong hands
- Bad actors trying to gain access

Security training and annual policy review

Ongoing training, starting at onboarding, sets the tone for expectations and reinforces your data security culture. It should apply to employees, contractors, third-party partners and anyone who might enter your premises or access your networks.

What it protects you from

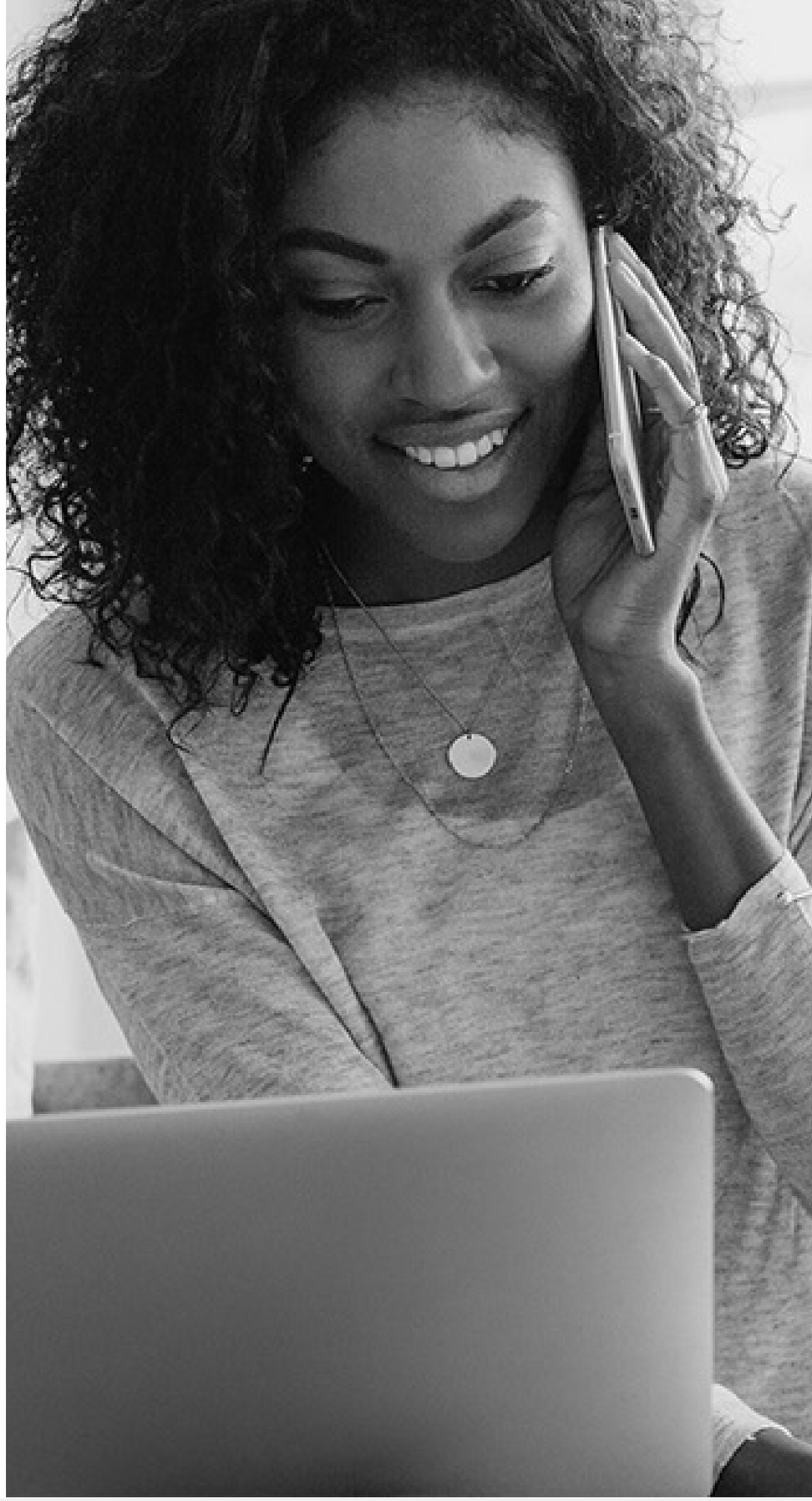
- Forgetful employees
- Unnecessary internal risk-taking
- Lack of knowledge about today's threats
- Careless storage of paperwork or digital assets

Where does the cloud fit?

Your cloud provider should be a trusted partner when it comes to the people that will be helping protect your data and applications. It is your organization's responsibility to ensure that your cloud provider's practices around policies, processes and training meet your own requirements. Here are a few things to ask about:

- Audits like SOC2, ISO27001, NIST800-53, PCI, FFIEC and others can help validate that the vendor is implementing best practice security procedures.
- Human resources security measures like background checks, confidentiality and non-disclosure commitments ensure the vendor's personnel is qualified to manage your data.
- Vendor management is important because the cloud provider may be sub-contracting many aspects of its operations to third parties, which must be adequately vetted.
- Continuous training of the vendor's staff ensures its employees are always prepared and certified on the newest threats, best practices and technologies.
- Annual policy review is critical to ensure the vendor is meeting its security program goals and its customers' requirements.

67 percent of breaches are caused by credential theft, social attacks like phishing and business email compromise, and errors.[iv]



layer 2:

PHYSICAL SECURITY

There's a reason defense in depth is sometimes called the 'Castle Approach.'

Fortification matters.

Physical security of your data might feel like an antiquated security protocol, but in fact it's critical to ensuring ongoing defense. Environmental threats and human threats are very real. If bad actors, water or fire — or any other host of unpredictable threats — can access your physical location and your system equipment, your entire enterprise is at risk. With an increasingly remote workforce and access to your data available through countless devices and applications, ensuring physical security is more important — and more challenging — than ever.

THE TAKEAWAY: Do everything you can to physically protect your data and devices, wherever they are.

Ready your physical access points »

WHAT GOOD PHYSICAL SECURITY LOOKS LIKE

Security guards

Guards provide the first line of physical defense at the data center and enforce advanced notice, proper identification and prior approval to get past the security desk.

What it protects you from

- Forced intrusions
- Unvetted employees, contractors or customers
- Corporate espionage

MFA, man traps and/or biometrics

These security measures help protect your facilities from access by unauthorized equipment or people.

What it protects you from

- Forced intrusions
- Unvetted employees, contractors or customers
- Corporate espionage
- Fraudulent primary credentials

Access control lists

Only guests on the master control list can be granted keys or code to sensitive areas within your facility.

What it protects you from

- Unvetted employees, contractors or customers
- Bad actors

Power redundancy

Uninterruptable power, even in the event of power grid outages, ensures your facility maintains top levels of security. This includes generators and the contracts for attaining the fuel required to continue operation.

What it protects you from

- Inaccessible data
- Network outages
- Ongoing loss of power

Fire suppression

Your fire suppression systems must be implemented in accordance with what is being protected. You may require different systems to protect your people, data and equipment.

What it protects you from

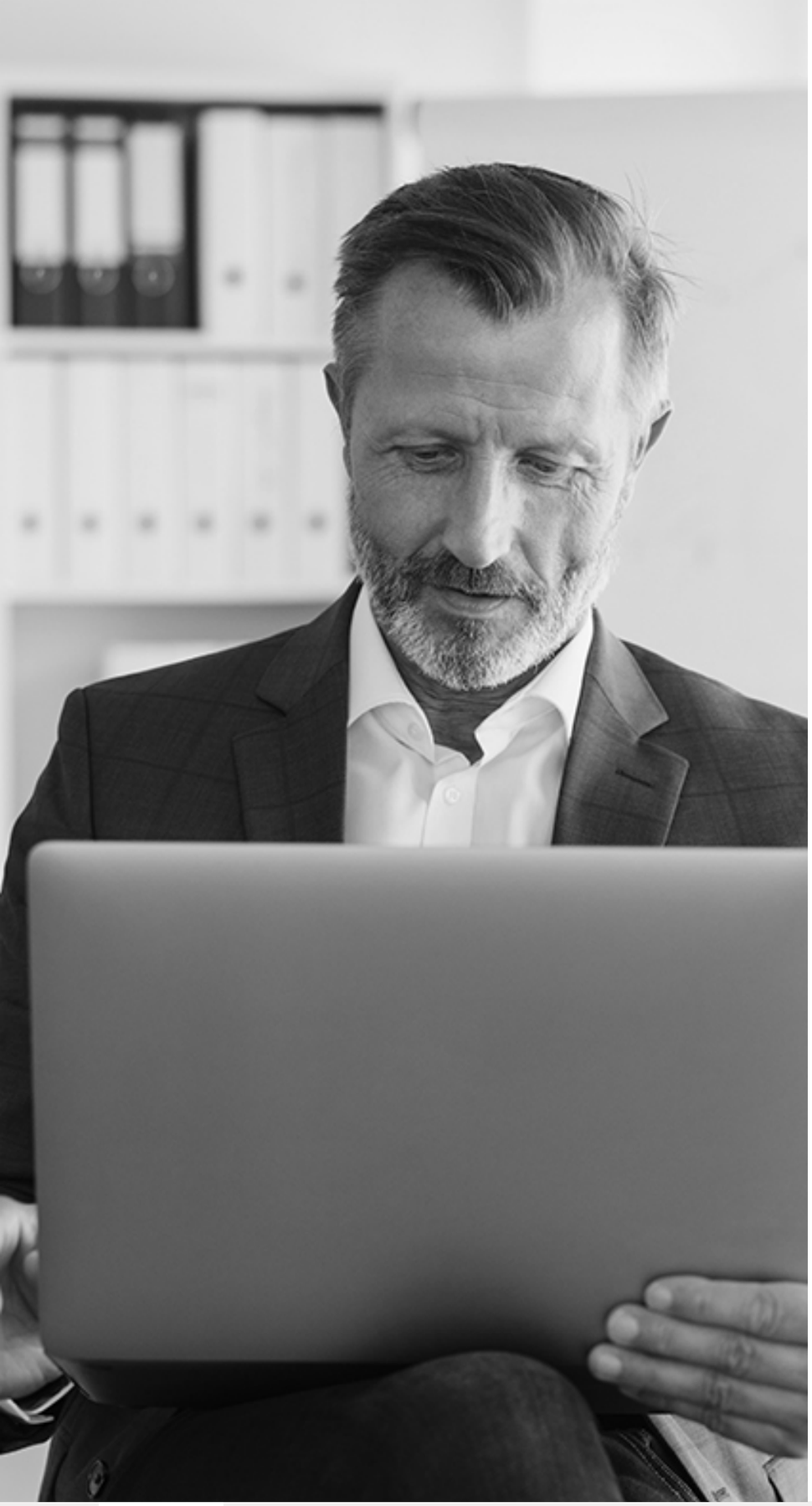
- Loss of data and equipment
- Inaccessible data
- Physical harm to on-site personnel

Geographic disbursement

Storing and backing up data across geographies increases performance and reliability, as well as protects applications and data.

What it protects you from

- Ensure availability despite natural disasters, such as storms and flooding
- Be prepared for power outages



Where does the cloud fit?

Whether you're looking to migrate to the cloud (like 58 percent of enterprises[v]) or re-evaluating your current cloud partner, physical security at your cloud data center must be an uncompromised priority. Just as you can take precautions to physically protect your data and devices, your cloud provider must do the same. The good news is that a well-established vendor in cloud delivery will often have better security than the average organization's on-premises strategy. In fact, 52 percent of business leaders say cloud deployment has the security advantage over on-premises storage[v]. Here are some things to research when evaluating cloud providers:

- Around-the-clock support is critical to provide hands-on operations with the hardware or the environment when needed.
- Security guards help deter and prevent an unauthorized user from entering the data center.
- Access control lists identify individuals with approved access and also log their entry and departure.
- MFA and biometrics access controls go a step further in validating only the right people can access the data center floor.
- Power redundancy provides uninterruptable power, even in the event of power grid outages, so the data center can maintain pinnacle levels of security.
- Fire suppression systems must be designed specifically for the data center to effectively prevent the fire from destroying data or compromising power and physical security.

> **10 percent of the year's breaches were motivated by espionage.[iv]**

layer 3:

PERIMETER DEFENSE

As our concentric circles get closer to the data, perimeter data defense looms into view. In the castle analogy, this is the moat — the first barrier to data breach by network.

If physical security protects your data from physical access to your facilities and devices, perimeter does the same for network access. Malicious actors will try to gain access to your environment. They're out there, searching networks and probing for weak spots, open ports and unpatched vulnerabilities that could be susceptible to their attacks.

When a sophisticated attack comes, the perimeter needs to absorb the first thrust. It needs to be able to parry attacks, monitor activity and automate improvement tactics to keep up with threats from the aggressive hacker community.

THE TAKEAWAY: A responsive perimeter defense will thwart initial attacks and discourage further attempts.

Monitor your network for perimeter incursions »

WHAT GOOD PERIMETER DATA DEFENSE LOOKS LIKE

Vulnerability and penetration testing

Penetration testing and regular vulnerability scans enacted by your security team allow them to understand public and internal vulnerabilities. Annual third-party penetration tests extend the security.

What it protects you from

- Nonsecure business processes and systems
- Lax security settings
- Malicious actors
- Unencrypted passwords and password reuse
- Unpatched vulnerabilities

Security Information and Event Management (SIEM)

A real-time analysis of security alerts generated by applications and network hardware, SIEM provides early attack detection while maintaining nonrepudiation logs to ensure data integrity.

What it protects you from

- Security events
- Early attacks

Early Denial of Service (DoS) attack prevention

Leveraging this service can provide early attack detection upstream of your environment, helping you keep your systems available to your users and customers.

What it protects you from

- Attacks that render machines or networks unavailable
- Superfluous requests that can overload the system and prevent legitimate requests from being filled

Next-Generation Firewalls (NGFW)

The third-generation of firewall technology combines traditional firewalls with other network device-filtering functions, including in-line deep packet inspection (DPI) and intrusion prevention systems (IPS).

What it protects you from

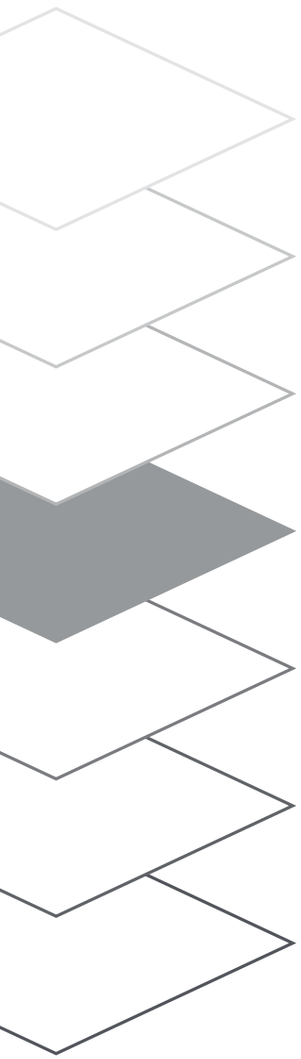
- Malicious activities
- Policy violations

Where does the cloud fit?

Today, your perimeter extends beyond the walls of your organization and can include remote and third-party environments. Your cloud provider can be a strong link in your perimeter defense, helping protect network access to the data center components. Ask your cloud provider to detail their perimeter defense strategy:

- **Vulnerability management and penetration testing** should be an extensive program including regular network vulnerability scans and externally performed penetration testing.
- **SIEM** should provide logging, monitoring and sophisticated early attack detection as well as measures for maintain nonrepudiation logs to ensure data integrity.
- **Secure admin access** should follow security best practices to adequately protect the vendor's admin access to your environment.
- **Early DoS attack detection** should be provided to detect and block attacks before they ever reach your systems.
- **Intrusion Detection System (IDS)/IPS** should include a range of advanced software and hardware solutions that monitor the network and systems for malicious activity or policy violations.

> Hackers attack every 39 seconds, on average 2,244 times a day.[vi]



layer 4:

INTERNAL NETWORK SECURITY

Beyond the perimeter defense is the formidable castle wall: The internal defense layer.

If hackers managed to breach the perimeter, their same strategy won't work here.

Hackers may get access to your internal network by many means, from highly technical to simply stealing access credentials from a legitimate user. Because your internal network connects so many critical devices and applications, this layer can be subject to attack more frequently than other more protected layers. But just because the hacker gets inside your network, does not mean that they will get easy access to your critical systems and data.

THE TAKEAWAY: The internal network security is a labyrinth of impediments that keep threats from getting close to their targets.

Reinforce your network with a secondary defense line »

WHAT GOOD INTERNAL NETWORK SECURITY LOOKS LIKE

Internal firewalls and network segments

Creating barriers between segments where security can be controlled is an extension of the diversified security strategy. For example, the web server segment shouldn't directly access the database segment.

What it protects you from

- Monitor and restrict access to prevent incursions

Encryption in transit

Encryption of data in transit is a critical component to a tightly secured environment. Externally, only encrypted traffic should be allowed into and out of the environment.

What it protects you from

- Protect solutions that require additional security levels, such as PCI compliance

Role-based access

Least-privilege protocols limit the systems that users and administrators can access, limiting the scope of damage if credentials are compromised.

What it protects you from

- Minimize the areas of potential compromise
- Mitigate risk of intentional or unintentional exposure by users and admins

Outbound web filtering

This limits the outbound traffic to known and approved channels and data types, ensuring attackers can't siphon your sensitive information.

What it protects you from

- Limit external exposure in case of a breach
- Prevent data exfiltration

High availability

Providing redundant configurations for critical systems ensures attackers or natural disasters can't easily take down the system, disable security protocols or destroy data.

What it protects you from

- Be prepared for natural disasters, such as storms and flooding
- Be prepared for unexpected power outages

Where does the cloud fit?

Your cloud provider should not only provide advanced internal network security at their data centers, but also effectively support your users and reinforce your organization's security protocols:

- **Internal firewalls and network segments** should provide secure barriers between functional areas of the data center, between your and other customers' environments, as well as between your solutions and services.
- **Data encryption in transit** should secure data traffic within the cloud environment and also between the cloud and your users and applications.
- **Role-based access** and least-privilege access protocols should apply not only to the cloud provider's own administrators, but should also be available to your organization's users and administrators.
- **Outbound web filtering** should be provided by the cloud vendor to protect your data from unauthorized exfiltration.
- **High-availability configuration** should provide N+1 redundancy for core components of your cloud service, ensuring not only uninterrupted access but also that all security measures remain in place even in the event of a component failure.

> Organized criminal groups were behind 55 percent of breaches.[iv]

layer 5:

HOST SECURITY

Your critical applications, services and components run on servers and other network hosts. With so many advanced technologies available for protecting your perimeter and your internal network, it may be tempting to skip over protecting your hosts.

That would be a big mistake.

Hosts can provide a robust layer of defense. Including host security in your defense-in-depth strategy will help ensure the systems running your applications, services and databases remain protected against attacks.

THE TAKEAWAY: Don’t relax your defenses — hardened hosts keep your critical applications running.

Don’t overlook your network hosts »

WHAT HOST SECURITY LOOKS LIKE

Endpoint detection and remediation

Tools like endpoint antivirus and malware detection can be very effective, even against new and unknown threats.

What it protects you from

- Detect and thwart malicious software

Hardened deployment

Only approved and necessary software should be deployed in the host system. This helps eliminate applications and settings that can create unnecessary security risks.

What it protects you from

- Prevent vulnerable applications from compromising the environment

Timely and responsible patching

All critical- and high-level patches should be addressed as quickly as possible (90 days or fewer is best practice). Patches should be put through a test environment before deploying.

What it protects you from

- Prevents known vulnerabilities from being exploited

Where does the cloud fit?

The cloud, of course, is made up of servers. And these servers and other hosts in the cloud provider's environment must be adequately protected. When done properly, your cloud environment can strengthen your overall level of security. Be sure to confirm the following with your cloud provider:

- Endpoint detection and remediation applications should be actively protecting the servers from malicious software.
- Hardened deployment methodology should be used to reduce risk of vulnerabilities.
- Patch management should be regular and proactive to limit risk from known vulnerabilities.
- Role-appropriate access should be given to server administrators, including your own.
- High-availability measures are used at host layer to ensure hosts remain secure and available to your users.

78 percent of business leaders say cloud deployment gives them an availability advantage over on-premises systems.[v]

layer 6:

APPLICATION SECURITY

Applications exist to give users convenient access to data. It is not surprising, therefore, that applications should include robust controls for ensuring only the right users get this access.

Application security is “the buck stops here” of your defense strategy.

All applications are not created equal, so it is critical to diligently vet your vendors or partners to assure they not only take defense as seriously as you do, but also have the experience, talent and agility to monitor threats and make updates to keep your application secure.

THE TAKEAWAY: Top-shelf content services solutions and the core line-of-business systems with which they interact should be armed with industry-leading defense.

Lean into the strength of your solution »

WHAT GOOD INTERNAL NETWORK SECURITY LOOKS LIKE

Secure application development lifecycle

Application security should not be just a bolt-on feature. It should start with the methodology used to develop, test and update software. Reputable software partners prioritize data security at every stage of the development process.

What it protects you from

- Reduce vulnerabilities in the application
- Enables the vendor to promptly address any future vulnerabilities

Encryption key management

Encryption at rest and in transit are fundamentals of data security, but both are moot if the encryption key isn't properly secured. Two methods of best practice key management include built-in encryption to the product and storage infrastructure — both inaccessible to admins.

What it protects you from

- Protect against nefarious admins
- Create hurdles for external threats

Access controls

One of the core factors in application security is ensuring only the authorized users can access the application and the data. This is accomplished through a variety of methods including group policies, the principle of least privilege, strong password policies, and integration with MFA, SSO and IDP services.

What it protects you from

- Protect against malicious actors looking for easy entry points
- Prevent accidental exposure and "privilege creep"
- Strengthen applications that have weak password requirements
- Easily implement robust methods of authentication for multiple applications

Application logging

Robust applications allow for logging so the customer can query/report on all types of access to data — viewing, changing, adding and deleting.

What it protects you from

- Ensure comprehensive audit trails
- Enable monitoring of applications

Unique application credentials

Application credentials should be separate from host or network credentials to provide an additional security barrier.

What it protects you from

- Prevent network and host admins from being able to access application data
- Keep proprietary enterprise data isolated from other parties

Where does the cloud fit?

A cloud provider that specializes in delivering your application can help enforce or strengthen customers' application security without introducing new risks or vulnerabilities into the equation. The following best practices can validate if your cloud provider is on the right track:

- **Encryption key management** should be done in the application, to eliminate the risk of an admin being able to compromise a key.
- **SSO** should be used for authentication into the cloud application to protect user credentials.
- **Annual penetration testing** should be used to not only protect the perimeter but also to detect application vulnerabilities.
- **Environment and application logging** should be enabled to provide your organization with complete visibility into access and changes to your cloud environment, your cloud applications and your data.

> "Taking content services to the cloud is about access to expertise across infrastructure, network security, compliance, application and platform development. For industries across the board, they're able to maintain the core competence of the business they're in, without having to worry about being experts in the infrastructure and hosting side of the equation."
>
> *Marc Cianciolo*
>
> *Director, Cloud Services, Hyland*

layer 7:

DATA SECURITY

This is it. The last stand in your seven-layer defense strategy.

Your actual data should be the most secluded and protected part of your environment.

Your data is at the core of your defense strategy. It is the very thing you want to protect the most. But that does not mean it has to be vulnerable if all the other layers are compromised.

THE TAKEAWAY: Multiple layers of defense apply to your actual data as much as they do to your strategy as a whole.

Harden your data's protection »

WHAT GOOD DATA SECURITY LOOKS LIKE

Encryption at rest

If data isn't being actively used, it should be encrypted.

What it protects you from

- Inappropriately accessed data remains protected

Data redundancy and replication

Production and backup data can replicated in more than one place to help protect it and to speed up disaster recovery.

What it protects you from

- Protect data from unrecoverable destruction due to a disaster or an attack
- Ensure data is available even during a disaster or an attack

Data separation

The data layer should be separated by network segments and firewalls from the rest of the infrastructure, and the only access allowed through should be the components that need direct access. Accessing layers should never be externally facing and should provide two or more layers before access.

What it protects you from

- Protect against unauthorized internal and external access

Least privilege access

As with the internal network layer, granting admins access only to what they need provides enhanced risk mitigation. Access to data should be reserved for the highest privilege tiers.

What it protects you from

- Nonessential parties can't access data they don't need

Where does the cloud fit?

When your data is stored in the cloud, your cloud provider should be your trusted first line of defense. There are numerous safeguards that should be in place to protect the data layer in addition to the ones already discussed in other layers. Here are some to keep in mind:

- **Encryption at rest** remains a simple but very effective way to protect data even if there is a breach. This may be provided by the application or the storage appliance itself.
- **Least privilege access** applies here to the provider's admins, ensuring they have minimal access to your actual data, or none at all.
- **Physical and logical separation** of your data in the data center ensures your data is separated from that of other customers by partitions, accounts, virtualization or physically; this reduces risk of unauthorized access or corruption.
- **Controlled accessibility** to the data layer is accomplished with intentional barriers like network segments and firewalls to ensure no direct and external access to the data layer.

> More than half of business leaders identify cloud security as an operational advantage over on-premises storage.[v]

Closing

Leveraging cloud infrastructure can effectively reinforce your overall defense-in depth strategy. Cloud technology has evolved dramatically, and today's cloud experts can provide features and defenses many organizations would have a difficult time matching on their own premises.

But of course, not all clouds are equal, and some are optimized for specific purposes. Choosing the right cloud provider can have both everyday and long-lasting impacts on the quality of your work and the lives of your employees and customers, not to mention the security of your data.

This is especially true when talking about applications that provide content services and process automation because they touch so much sensitive data and so many critical systems. If a cloud provider is not prepared to meet your security requirements, the long-term health of your enterprise could be at stake.

Delivering content services applications in the cloud is about more than just finding a new place to store your data. It can provide an environment that is specially built and optimized to meet your needs — ever-increasing data, incomparable security, ease of use for customers and employees and an expert partnership to support you along the way.

Your organization's future depends on today's decisions.

Start fortifying today!

Want to learn more about security of the Hyland Cloud and our industry-leading content services?
Visit Hyland.com/Cloud

Hyland®

Learn more at **Hyland.com/Cloud**

i. Ponemon Institute, Cost of a Data Breach Report 2020, 2020.

ii. Ponemon Institute, 2017 Cost of Data Breach Study, 2017.

iii. GDPR, What are the GDPR fines?

iv. Verizon, 2020 Data Breach Investigations Report, 2020.

v. IDG, Content services: leveraging cloud for improved IT and business outcomes, 2018.

vi. University of Maryland, Study: Hackers attack every 39 seconds, 2007.