HOW THE CLOUD CAN FORTIFY YOUR SECURITY

Nearly 80 percent of senior IT and IT security leaders believe their organizations lack the protection they need to thwart cyberattacks — despite increased IT security investments recently made to combat changing work dynamics.[1]

How can visionary leaders enable the security environment they need?

For many, the answer is in moving to the cloud (or to fortifying their position there).

But, just putting something in the cloud doesn't make it safe. Most organizations only truly adopt best-practice cloud security when they partner with a cloud provider that expertly executes the common IT security strategy called defense-in-depth.

Defense-in-depth spreads diverse security mechanisms across seven layers, including in the cloud, so that even if one layer fails, there are six others offering a strong — but different — defense.

Here's what it takes.

Layer 1 POLICIES, PROCEDURES AND AWARENESS

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

67%

BREACHES CAUSED BY CREDENTIAL THEFT, HUMAN ERRORS, AND SOCIAL ATTACKS LIKE PHISHING AND BUSINESS EMAIL COMPROMISE[2]

CLOUD COMPONENT

- Cloud provider meets or exceeds your own policies and procedures
- Third-party audit-certified, like SOC2, ISO27001, NIST800-53, PCI and FFIEC
- Strong HR security measures, vendor management and continuing training

Layer 2 PHYSICAL SECURITY

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

10%

BREACHES MOTIVATED BY ESPIONAGE[3]

CLOUD COMPONENT

- Around-the-clock support and security guards for the data center
- Access controls, such as lists, multifactor authentication (MFA) and biometrics
- Power redundancy and fire suppression systems

Layer 3 PERIMETER DEFENSE

When a sophisticated attack comes, the perimeter needs to absorb the first thrust.

$1 trillion

ESTIMATED GLOBAL LOSSES FROM CYBERCRIME[4]

CLOUD COMPONENT

- Vulnerability management and penetration testing
- Security Information and Event Management; early DoS attack detection
- Secure admin access protocols

Layer 4 INTERNAL NETWORK SECURITY

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

55%

BREACHES CONDUCTED BY ORGANIZED CRIMINAL GROUPS[3]

CLOUD COMPONENT

- Internal firewalls and network segments
- Data encryption in transit
- Role-based and least-privilege access protocols
- Outbound web filtering
- High-availability configuration with N+1 redundancy

Layer 5 HOST SECURITY

Don't relax your defenses — hardened hosts keep your critical applications running.

78%

BUSINESS LEADERS WHO SAY CLOUD DEPLOYMENT GIVES THEM AN AVAILABILITY ADVANTAGE OVER ON-PREMISES SYSTEMS[5]

CLOUD COMPONENT

- Endpoint detection and remediation applications
- Hardened deployment methodology
- Regular and proactive patch management

Layer 6 APPLICATION SECURITY

All content services solutions and the core line-of-business systems with which they interact should be armed with industry-leading defense.

76%

BUSINESS AND IT DECISION-MAKERS WHO SAY APPLICATION SECURITY IS A TOP PRIORITY[1]

CLOUD COMPONENT

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.

- Encryption key management at the application level
- SSO for authentication into the cloud application
- Environment and application logging for a complete view into access and changes in the cloud environment, cloud applications and data

Layer 7 DATA SECURITY

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

91%

IT LEADERS WHO SAY THEIR CYBERSECURITY BUDGET INCREASED THIS YEAR[1]

CLOUD COMPONENT

- Encryption at rest
- Controlled accessibility to the data layer with intentional barriers like network segments and firewalls
- Physical and logical separation of your data from other cloud customers' by using partitions, accounts, virtualization or physically

ACHIEVING DEFENSE-IN-DEPTH

What's the best path forward?

Implementing and maintaining these security protocols can be so resource-intensive and complex that it can be difficult to know where to start. Perhaps more concerning, if an existing cloud deployment isn't properly configured and maintained, your organizational security could be at heightened risk.

The go-forward: A proven partner can help you achieve true cloud security and is the best route for most enterprises that don't want to dedicate complex expertise or limited bandwidth to security management. Hyland has built every layer of the defense-in-depth model into our cloud offering, the Hyland Cloud.

THE HYLAND CLOUD

The Hyland Cloud is a secure, privately managed cloud platform that is custom-designed to host **content services** for Hyland customers. More than 1.2 million Hyland Cloud users accelerate their business growth there, and a recent **Forrester**[vi] report uncovered the following about Hyland customer results:

ROI	SPEED	PRODUCTIVITY
293%	Content services were built **75 percent** faster	**50 percent** increase in end-user productivity

"We've hosted solutions before, and we knew we didn't want to be in the data center business. It's expensive and difficult. Managing a server is a job in and of itself. What if something happens and the server gets destroyed? We wanted to know with certainty that the data was being cared for outside of our building."

Bob Walters
Business Analyst and OnBase System Administrator
Heinen's | Get the full story

Learn more about **our safe, secure and reliable cloud platform here**

1. IDG and Insight, Cybersecurity at a crossroads, 2021.
2. Verizon, 2020 Data Breach Investigations Report, 2020.
3. IBM, Cost of a Data Breach Report, 2020.
4. IDG, Content services: leveraging cloud for improved IT and business outcomes, 2018.
5. Frost & Sullivan, Your business shortcut to digital transformation, 2020.
6. Forrester, The total economic impact of content services in the Hyland Cloud, 2020.

Hyland