

AHEAD



# Securing the Enterprise:

## A Maturity Model for Cybersecurity



# Six Challenges Enterprise Security Professionals are Facing Right Now

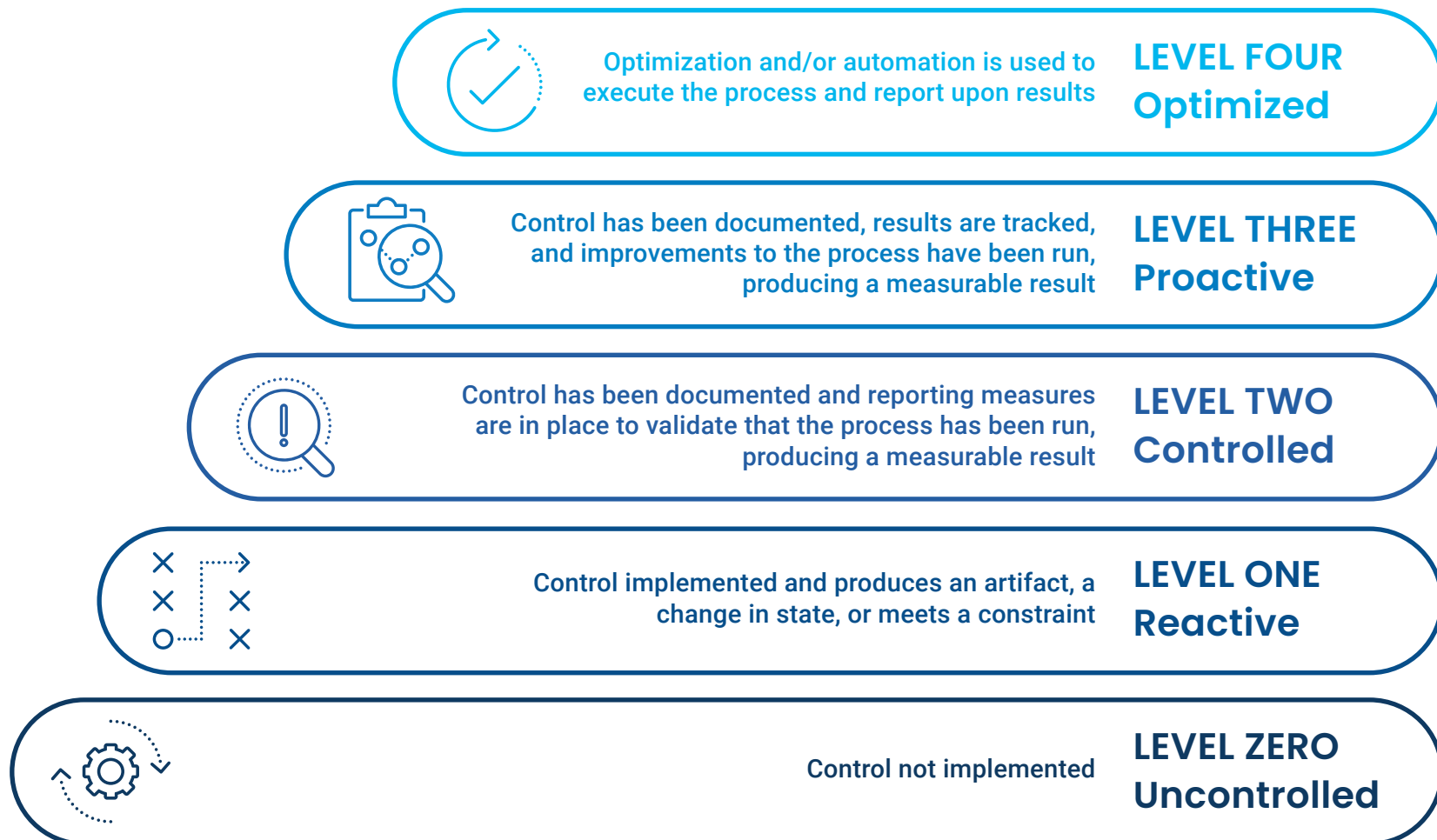
- 1 Adoption of the Public Cloud is No Longer an Option
- 2 Ransomware Cyberattacks are Skyrocketing
- 3 A Shortage of People and Skills Continues to be a Problem
- 4 The New Way to Work is Affecting Application Delivery
- 5 Corporate Compliance Programs Continue to Fail
- 6 Security Maturity: No Direction Equals No Prioritization

## The First Step: Prioritize & Act

With an ever-increasing number of security concerns to consider, organizations must base prioritization on the most significant benefits across multiple challenges. By understanding the most common tactics, techniques, and procedures used by attackers, enterprises can more effectively assess their current state and prioritize action.

# How Mature are Your Security Processes?

Like building a house, a security program is best developed in stages. While it's easy to focus on building the visible and more 'flashy' elements of a program, it's the foundational elements that provide structure and protect against the most common threats. A maturity-based approach grants structure to your program, allowing you to not only project your estimated protection level but more easily plan for the financial and staffing implications of your decisions.



# Security Solution Maturity Mapping

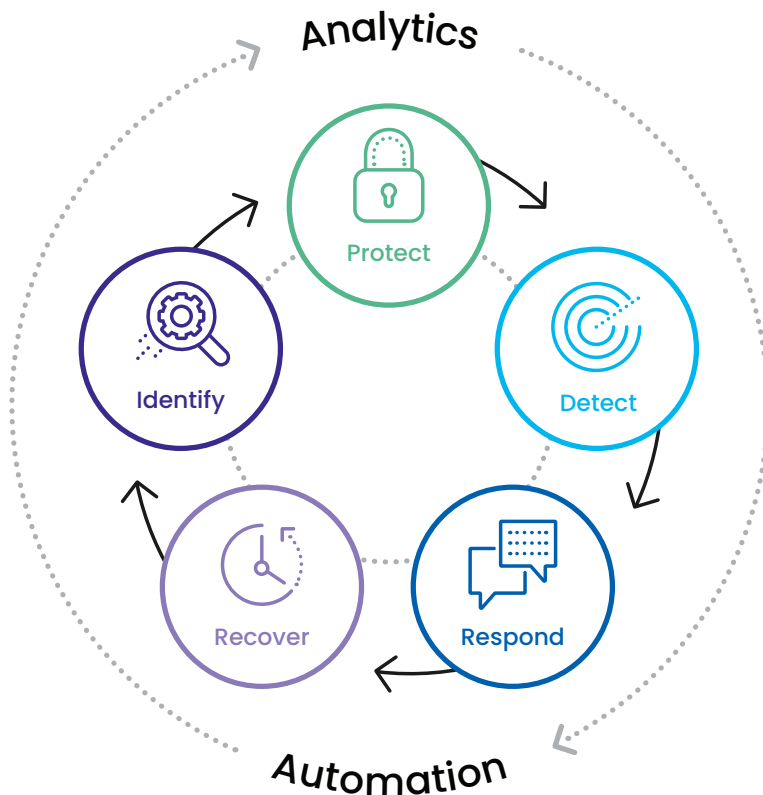
To build a regimented security program, it's essential to follow a path that leverages known controls against your anticipated threats. Foundational elements like user education and security awareness training should be part of every program. By building upon the essentials, you not only satisfy the requirements of your compliance frameworks but foster resilience in the form of redundant and adaptable controls. This 'Defense in Depth' model also allows organizations to tailor the controls to fit the organizational risk appetite and plan more effectively for security budgeting cycles.

| MATURITY LEVELS                  |                                                           |                                                          |                                                                  |                                                                                        |
|----------------------------------|-----------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------|----------------------------------------------------------------------------------------|
|                                  | 1<br>REACTIVE                                             | 2<br>CONTROLLED                                          | 3<br>PROACTIVE                                                   | 4<br>OPTIMIZED                                                                         |
| Phishing                         | Education & Awareness                                     | Anti-Phishing Solution                                   | Phish Testing                                                    | Phish Testing w/<br>Automated Training                                                 |
| Web-Apps                         | Web Application Firewall<br>DNS filtering                 | Application Testing<br>Web Access Filtering              | Breach Testing                                                   | Continuous Breach Testing                                                              |
| Endpoint Protection              | Anti-Malware                                              | Managed Anti-Malware                                     | EDR Solution                                                     | Managed EDR Solution                                                                   |
| Privilege Escalation             | Local Admin Password<br>Solution (LAPS)                   | Privileged Account<br>Management (PAM)                   | Privileged Account<br>Management (PAM) w/<br>Workflow Management | Identity Governance<br>Program w/Automation                                            |
| Lateral Movement<br>(Zero Trust) | Identity<br>Local Admin Password<br>Solution (LAPS)       | Privileged Account<br>Management (PAM)                   | PAM w/ Workflow<br>Management                                    | Identity Governance<br>Program w/Automation                                            |
|                                  | Network<br>Blacklist model - Prod/Dev/<br>Test separation | Compliance Based<br>Segmentation                         | Hybrid Black/Whitelist<br>Critical App Segmentation              | Full Whitelist Model Full<br>App Segmentation                                          |
| Data Encryption                  | Anti-Encryption w/Alerting                                |                                                          |                                                                  | Anti-Encryption w/Analytics<br>and Automation                                          |
| Data Loss                        | Immutable Backups                                         | Single Channel DLP<br>Multifactor Delete<br>Confirmation | Single Channel DLP<br>Analytics w/ Anomaly<br>Detection          | Multi-channel DLP w/ Monitoring<br>and Kill Switches<br>Air-Gapped Backup w/ Analytics |

# Where to Focus – NIST Cybersecurity Framework

The key to enhancing your enterprise security maturity involves setting a strategy, translating it into an executable process that works to reduce manual workload and drive efficiency, and validating all outcomes to verify that the desired results are being met. By adopting a holistic approach to enterprise security, organizations can ensure that automation, analytics, and agile thinking are being applied across the full security lifecycle.

## Security Lifecycle



### IDENTIFICATION

AHEAD will help implement a robust vulnerability management program, giving you the insights you need to prioritize risks across your environment.

### PROTECTION

AHEAD can employ an in-depth strategy to protect your organization from attacks.

### DETECTION

AHEAD will tap the insight and power of your log data across all systems, as well as network and privileged user monitoring, to detect anomalies and respond faster.

### RESPONSE

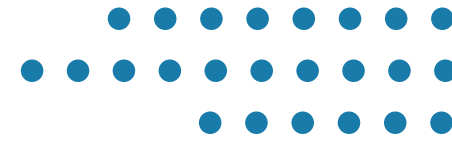
AHEAD will lean on its deep roots in automation and enterprise service management, to quickly prioritize threats and automate the response to frequent and common security events.

### RECOVERY

AHEAD will leverage its heritage of robust backup solutions to ensure minimal disruption to your business and protect your data in the public or private cloud.



# AHEAD's Approach to Cybersecurity



## Ready to Enhance your Organization's Security Strategy?

Contact AHEAD to learn how our enterprise security experts can help you mature your security programs to safeguard your organization from attacks and leave you better prepared for the future.

### About AHEAD

AHEAD builds platforms for digital business. By weaving together advances in cloud infrastructure, automation and analytics, and software delivery, we help enterprises deliver on the promise of digital transformation. To learn more about our approach to enterprise digital transformation, send a note to [contact@ahead.com](mailto:contact@ahead.com).

# AHEAD

**Learn. Grow. Achieve**

© 2021 AHEAD Inc. All Rights Reserved.

## National Hubs

### ATLANTA

1117 Perimeter Center  
W406  
Atlanta, GA 30338

### CHICAGO

401 Michigan Ave.  
#3400  
Chicago, IL 60611

### SAN FRANCISCO

2000 Crow Canyon Place  
Suite 250  
San Ramon, CA 94583

[www.ahead.com](http://www.ahead.com)