A Guide to Integrated Security
Digital Business Continues to Move the Cyber Goal Posts

Fortune magazine estimates that by the year 2020, US companies will spend $101 billion per year on cyber security, up 38% from 2016. With all of the money being invested in cyber security, why do the pace and complexity of new security threats continue to rise year after year?

A big reason is that today’s digital business involves a more mobile workforce with expectations of immediate and on demand access to data fronted by intuitive and engaging user experiences, and often underpinned by public cloud infrastructure for increased agility and time to market.
In the past, traditional security teams didn’t even have the resources at their disposal to defend data center infrastructure and user populations. Security organizations are especially stretched these days - lacking the time and education to keep up with the pace of innovation amongst threats.

Traditional firewalls protected the network edge, but a mobile workforce has destroyed the perimeter. Data used to be stored safely inside the data center network, but now RESTful API are made public, potentially exposing corporate data. Meanwhile, the cloud brings with it a new set of skillset requirements for both IT and Security engineers. Concerns over the public exposure of S3 buckets simply didn’t exist in traditional IT (see Figure 1.)

Companies must pay down their technical debt, and legacy applications weren’t designed to operate cost effectively in the public cloud. Security teams are constantly fighting to secure out-of-date operating systems and applications that may no longer be supported. This leads directly into our final point of why many organizations are struggling with security; poor hygiene.

As security expert Bruce Schneider says, “If you’re focusing on what’s in the news you’re focusing on the wrong thing. Something that happens so infrequently that it makes the broadcast news, tells you that you shouldn’t worry about it.” The reality is that most security issues occur because of poor IT hygiene. Consider the incredibly damaging Equifax breach. It came down to a poor job of patching.

Vulnerability management, a key pillar in any information security program seems simple. But as we’ve already noted, many companies use platforms that are out of date, and applying patches isn’t an option. In other cases, an application vendor will support the most up-to-date version of a dependency. This business is faced with a lose - lose situation; patch and cripple their business, or don’t patch and leave vulnerabilities exposed to attackers. Finally, from a vulnerability management perspective, teams often lack the knowledge to properly prioritize their vulnerability remediation. A system buried deep in the corporate network behind several pairs of firewalls isn’t as critical as the same vulnerability providing web services publicly exposed on the Internet.
A mobile, demanding workforce has destroyed the perimeter

Security teams constantly fight to secure out-of-date systems

Most security issues occur because of poor IT hygiene

Teams lack time and knowledge to prioritize vulnerabilities
A Closer Look at the Current State of Cyber Security

For a look at just how critical these vulnerabilities are in reality, the Verizon Data Breach Incident report serves as an excellent resource. Figure 2 shows an excerpt from the 2018 report.
In looking at this data set, you’ll notice some disturbing trends about the security industry. In most cases, compromises happen within minutes. Once an attacker has accessed the network, data exfiltration begins in a few minutes - perhaps a few hours.

The most alarming finding is that organizations don’t discover they’ve been breached until months later, and to clean up an
Establish Security Guardrails, Not Roadblocks

So how can you address such systemic issues? Part of the problem organizationally is that too many security activities - and sometimes the CISO role itself - operate in isolation from the rest of the organization. Security is not just a CISO issue, as you saw from the examples of poor patching and hygiene being a key cause of breaches. All of IT and business leadership need to stay involved. Rather than disconnected security programs, strive for what AHEAD calls Integrated Security – the systematic inclusion of security planning and activities in every process and project.

The objective is not to set up roadblocks - as security functions can sometimes do - but instead to provide the guardrails that allow the business to move faster, yet safely.

Infrastructure and operations teams face the challenge of understanding new cloud operating models, and security teams need to be arm-and-arm with them. The most successful security teams are completely aligned and integrated with the rest of IT and the business. We observe four integrated security habits within our customers that make them successful.

Successful security teams:

1. Are aware and supportive of the business’s plans and adapt early to support them.
2. Work closely with the technology or enterprise project management office early on during project vetting and planning.
3. Have abandoned the “shiny object” mindset and have started to adopt risk- and process-based security programs.
4. Prioritize investments in security automation in order to manage the onslaught of events they face.
Two Examples of Integrated Security

▶️ One AHEAD client operates the fifth largest e-commerce platform in the world. One of the reasons they’re known to have such an outstanding Integrated Security model, is because their security team is actually embedded in the project management office.

Every time the company initiates a new project, someone from security is evaluating that project from the outset: What type of data will be stored? Is it our customer’s credit card data? Is it our user database? Is it our financial records? The security analyst assesses the associated risk and identifies the required controls to put in place.

▶️ Another stellar example of Integrated Security comes from a technology company and how they integrate security into their application development processes.

When it comes to application security, most companies just buy a code scanner, which assesses the code, allowing the team to issue tickets for their developers to fix.

The company in question operates very differently. When they hire someone new onto their security team, they actually hire software developers, not security experts. They educate those developers on how to write secure code, and then charge those developers to train their other software development teams.
Integrated Security Means Applying Automation and Analytics Holistically

Infrastructure and operations teams face the challenge of understanding new cloud operating models, and security teams need to be arm-and-arm with them. The most successful security teams are completely aligned and integrated with the rest of IT and the business. With a fully integrated approach, teams can apply automation, analytics, and agile thinking across the entire security lifecycle (see Figure 3.)
FIGURE 3
Integrated Security Lifecycle

- Protect
- Detect
- Respond
- Recover
- Identify
- Analytics
- Automation
**Identify**

Implement a robust vulnerability management program giving you the insight you need to make prioritized decisions where risks are in your environment.
Protect

Put a comprehensive strategy in place to protect your organization from attacks, for example, using network micro segmentation to reduce your attack surface.
Detect

Tap the insight and power of your log data across all systems to detect anomalies and put you in a position to respond in a timely manner.
Respond

Apply automation relentlessly to help quickly prioritize threats and automate the response of frequent and common security events.
Recover

Apply robust backup solutions to ensure minimal disruption to your business and keep your data in the public or private cloud, safe.
Where Integrated Security Matters Most

Let’s discuss the solution aspects of Integrated Security. To do that, we must work our way across other areas of IT and other digital imperatives. Next are the technology building blocks to a comprehensive Integrated Security program.
Security Operations

Most scaled security operations programs consist of three key capabilities: Vulnerability Management, Incident Response, and Threat Intelligence.

- Vulnerability Management ingests data and reports the state of your IT hygiene to technology and business leaders alike.
- Threat Intelligence replaces manual web searches and loads of emails, with automated feeds that inform you of threats - putting it in one place for a SecOps team to consume.
- Incident Response can use automation to trigger defined processes that run when an incident - like a phishing email - is recognized. One energy sector client of AHEAD estimated that they could eliminate 4 to 8 hours of manual effort for each phishing email response. And this company receives hundreds of phishing emails each day.

When automation is added to the security mix, the busy work of your security analysts can be eliminated, freeing them to improve security processes or introduce new security capabilities.
Governance, Risk and Compliance

This capability supports the review and validation of controls that need to be in place, including an attestation that the controls are effective. Again, security often comes down to poor IT hygiene, and poor patching is a prime example of a behavior that requires better controls.

In the patching example, GRC can help track how quickly you’re patching vulnerable systems, couple it with data from the CMDB, and tie it back to the SecOps module to report back to the business a state of compliance.
Cloud Security

When organizations establish their public cloud foundation, they’ll first look to ensure the proper security and controls are in place as prescribed by their cloud provider. But are those workloads ready for a compliant-based environment where PHI, PII, PCI data might live? The answer is too often, “No.”

You’re responsible for vulnerability management, threat intelligence, and incident response in the public cloud, the same way you are with on-premises. And in certain cases, the level of protection will not be met by the foundational services provided by the cloud providers.
Application Development

Security needs to be an integral part of the Scaled DevOps imperative, as evidenced by DevSecOps now becoming a popular term.

In software development, security is often a supply chain problem. It’s now common for hackers to attack GitHub repositories with malicious code, which then finds its way into thousands of enterprise application portfolios.

Security has to play a prominent role across your DevOps Toolchain, with the ultimate goal being the automation of security policy configurations.
A Maturity Model for Integrated Security

Corporate efforts around security detection, response, and remediation are still immature, challenged to keep up with digital business demands.

Some companies are digital natives, writing software for a living, and therefore understand the interdependencies of their applications. Along with the fact that they have less technical debt than most enterprises, they’re pretty advanced with respect to integrated security.

But consider a lot of enterprises, such as those in healthcare. They’re rolling out biomed devices, and don’t have a clue as to what those biomed devices talk to. They’ve got large applications like EPIC and medical imaging systems, with little insight into what ports and protocols these assets use to communicate on the network. They have many legacy apps that are used to run the business, and their vendors don’t support those applications very well.

All of this technical debt complicates IT hygiene, and makes Integrated Security a journey, not a sprint. As with all of our Digital Delivery Platform imperatives, AHEAD created a 5-stage maturity model to help guide your Integrated Security journey and monitor your progress (See Figure 4.) We used ISO33004 as a reference and applied the COBIT CMMI stages to each of 20 CIS controls (See Figure 5.)
FIGURE 4
Maturity Model for Integrated Security

STAGE 0
Absent

STAGE 1
Ad Hoc

Control implemented and produces an artifact, a change in state, or meets a constraint

STAGE 2
Procedural

Control document and reporting measures are in place to validate

STAGE 3
Managed

Results tracked and improvements run, producing a measurable result

STAGE 4
Automated

Automation is used to execute the process and report upon result trends
### FIGURE 5

CIS Controls Applied in the Integrated Security Maturity Model

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>Inventory</td>
<td>Continuous</td>
<td>Controlled</td>
<td>Secure</td>
<td>Maintenance</td>
<td>Email and Web Browser</td>
<td>Malware Defenses</td>
<td>Limited</td>
<td>Data Recovery</td>
<td>Secure Configuration</td>
<td>Controlled Access</td>
<td>Wireless Access</td>
<td>Account Monitoring</td>
<td>Security Awareness</td>
<td>Application Software</td>
<td>Incident Response</td>
<td>Penetration Tests</td>
</tr>
<tr>
<td>and Control</td>
<td>and Control</td>
<td>Vulnerability</td>
<td>Use of Admin</td>
<td>Configuration</td>
<td>Monitoring and Analysis</td>
<td>Protections</td>
<td>and Services</td>
<td>and Control</td>
<td>Capabilities</td>
<td>for Network Devices</td>
<td>Based on Need to Know</td>
<td>Control</td>
<td>and Management</td>
<td>and Training Program</td>
<td>Security</td>
<td>and Management</td>
<td>and Red Team Exercises</td>
</tr>
</tbody>
</table>
Targeted Areas Where AHEAD Can Help

Based on client demand, AHEAD has developed these specialized offerings designed to help you along the Integrated Security journey.

Integrated Security Visioning Workshop

In this executive workshop designed to bring together the CISO and CTO, we report out our assessment of your current security environment, processes, and architecture – then facilitate a new course along the CMM maturity continuum.
AHEAD helps many clients establish the right public cloud foundation, but these often are limited to non-compliant workloads. The Cloud Security Foundation extends your foundation to address all things in the CIS domain, as well as applying vulnerability management, threat intelligence, and incident response to your public cloud environment.
Secure CMDB Foundation

AHEAD also helps many clients construct their CMDBs. Similar to Cloud Security Foundation, our Secure CMDB Foundation brings a security perspective to populating your CMDB, including how to enforce proper infrastructure configuration throughout.
Vulnerability Management Foundation

This foundation serves as an initial engagement to set up a client with the right vulnerability process and approach to identifying and prioritizing vulnerabilities on a continuous basis.
Integrated Security is one of five imperatives that comprise the AHEAD Digital Delivery Platform.

The other imperatives are:
- Relentless Automation
- Intelligent Operations
- Scaled DevOps
- Enterprise Cloud