ActualTech Media

UncommonX

What Does a Holistic Security Solution Look Like?

Lawrence Miller

CONTENTS

IN THIS PAPER

Learn how a holistic security solution can help organizations validate, prioritize, enrich, and correlate information for an end-to-end awareness of related threat activity and improve their ability to prevent threats.

Highlights include:

- Establishing a baseline to understand business services and data flows so that anomalies can be identified
- The three most important components of a holistic security solution: security maturity, industry comparison, and change over time
- How the UncommonX BOSS intelligent security platform can help your organization to mitigate and guard against threats

Cybersecurity risks are unique among technology challenges in that they can come from any and every part of your environment. There are thousands of tools that claim to solve cybersecurity issues, yet many of them have huge problems themselves. This is why even the largest organizations overinvest in security technologies. They buy tools, then they buy more tools to manage the tools—and they invest in recruiting and retaining security teams (including offshore talent), which is increasingly difficult in an increasingly competitive job market that has a severe shortage of available qualified security professionals.

> **A new type of security operations platform is needed—a holistic security solution—that works *with* your existing tools.**

Clearly, a better approach to security is needed. But no organization can afford to simply toss out its existing security infrastructure and tools and replace them with the "latest and greatest" security innovation. Instead, a new type of security operations platform is needed—a holistic security solution—that works *with* your existing tools to validate, prioritize, enrich, and correlate information for an end-to-end awareness of related threat activity and improves their ability to prevent threats.

Fact-Based System

The first key to a holistic security solution is ensuring you can quickly and automatically create an accurate inside-out view of all your IT systems, applications, services, and resources. This information provides the necessary context to sort real risks from noise in your environment.

One thing distinguishing a holistic security solution is that it's a fact-based system. It creates a baseline that's predicated on gathering information directly from the device. The goal of the baseline is to understand the business services and data flows so that anomalies can be identified later. The solution actually touches every endpoint in your environment, logs in, and runs commands on that endpoint to collect information such as make, manufacturer, installed operating system, patch level, local users, and more. Assets are further processed into a host classifier, where it's designated as a Windows, Linux, or network system. From there, a logical grouping of hosts is created based on their role, function, services, and relevance to the business.

In contrast, most security tools simply infer device information from a firewall signature or make assumptions based on how similar devices have responded to a particular request type. Anything inferred is guessed—so it will not stand in a court of law. And let's be clear: cyberattacks are most often perpetrated by cybercriminals. A cyberattack may lead to criminal prosecution, civil litigation, or regulatory non-compliance actions. That means there's a good chance you'll end up in court after a successful cyberattack, so your forensic information needs to be fact-based to ensure it can stand as evidence.

> **The goal of the baseline is to understand the business services and data flows so that anomalies can be identified later.**

On a network level, it's assessing the IP stack's response. This has become hugely difficult in hyperconverged infrastructure, in which you have one physical network controller responding for as many as 400 virtual devices.

Relevance

An essential challenge for security and IT executives is making security relevant to the business by putting security into terms that your other business leaders can understand (read "The Business Case for Security" to learn more about putting security into business terms). Business discussions about risk are focused on potential impact (in dollars), the cost of limiting risks, industry comparison (including comparative situations with actual breach cost), and change over time. Therefore, the

three most important components of a holistic security solution that will help you make security information relevant to your business are: security maturity, industry comparison, and change over time.

You can think of the three measures of relevance in terms of a top-down framework. It starts at a macro-level (NIST Cybersecurity Framework), then drills down to industry norms (industry comparison), and finally tracks your organization's progress toward specific goals (change over time).

SECURITY MATURITY

A security risk maturity assessment (see **Figure 1**) helps an organization understand where it is (current state or "as is") and where it wants to go (future/desired state or "to be"). A security risk maturity assessment helps organizations:

- Reduce security threats by uncovering vulnerabilities
- Inventory all assets and identify any unknowns
- Ensure security and business objectives are aligned
- Verify regulatory compliance requirements

Although the organization can perform a maturity assessment itself, it's often better to work with a third-party to assess your capabilities independently and objectively across a broad spectrum of criteria.

The three most important components of a holistic security solution that will help you make security information relevant to your business are: security maturity, industry comparison, and change over time.

Leveraging a third-party will also help you ensure you set practical short-term and long-term goals for your desired future state. For example, not every organization needs to be "world-class" (or some similar top-level maturity) in every aspect of its risk management program and there is a cost associated with achieving various levels of maturity.

INDUSTRY COMPARISON

Security and compliance are a journey and achieving a benchmark or standard doesn't happen overnight; maintaining a given risk or compliance posture requires ongoing diligence.

For many organizations, understanding how you compare to and sharing relevant information with your peers is a helpful metric. The nature of risks and threats facing an organization in the healthcare industry, for

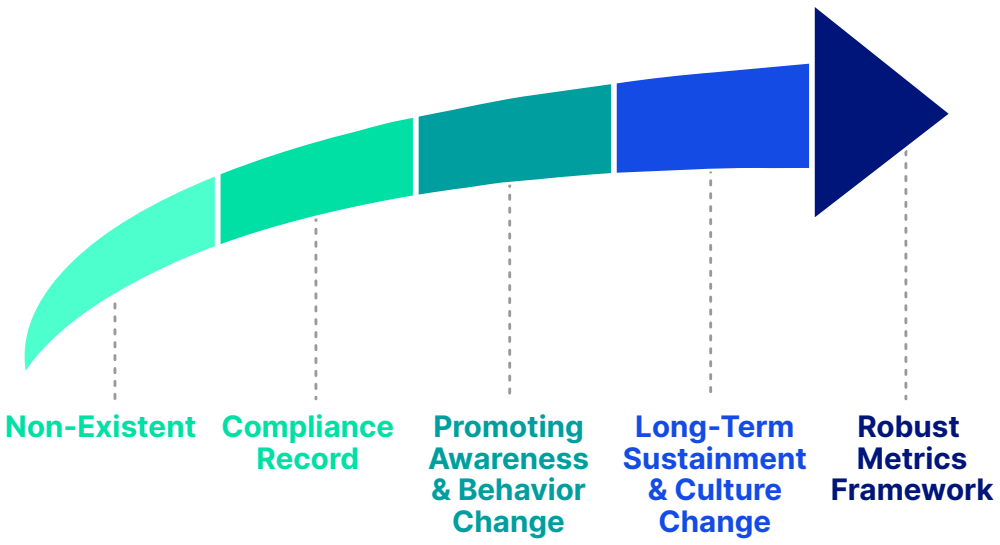

Figure 1: Security awareness maturity model

example, will be somewhat different from those experienced by an organization in the retail industry. There are unique systems and data to be protected across these vastly different industries, and different business priorities and resources available in each industry.

An industry percentile—calculated using data from industry sources, open-source commercial intel, and other sources—can provide business executives with a relevant measure to assess what's normal and appropriate for their unique industry.

> **Security and compliance are a journey and achieving a benchmark or standard doesn't happen overnight; maintaining a given risk or compliance posture requires ongoing diligence.**

CHANGE OVER TIME

Finally, within your own organization, it's important to track your progress toward a "desired state" risk posture over time. Tracking progress at a granular level, such as week-by-week, helps instill a culture of continuous improvement within your organization.

SAAS AND MSSP

Many organizations are turning to Software-as-a-Service (SaaS) offerings or managed security service providers (MSSPs) to address some or all of their organization's security needs. When considering SaaS or an MSSP, the business must understand its risks and tolerance in relationship to the resources these options can apply to mitigate the risks. SaaS solutions and MSSPs have their own inherent risks which must also be considered and mitigated, typically through validation by audit, certification, or both.

Ultimately, you're still responsible for your organization's risk, so it's critical that you validate any SaaS or MSSP offering to ensure it can meet your needs. You must be certain your provider is someone you trust as a partner on security for the long haul.

> **You must be certain your provider is someone you trust as a partner on security for the long haul.**

Get Strategic with Your Security

UncommonX offers unmatched enterprise-class cybersecurity protection for mid-size organizations by combining adaptive threat and intelligence software with 24/7 industry experts, making it easy to constantly both map and fix root causes of security vulnerabilities. Taking a market-first inside-out approach to ongoing digital security risks through unique curated threat feeds and automated analytics, the UncommonX BOSS intelligent security operations platform provides clear contextual awareness to yield accelerated outcomes to mitigate and guard against threats. Learn more at UncommonX.com.