



The Importance of Proactive Security

Mark Sangster

In This Paper

Defending your network against highly motivated and well-equipped threat actors requires a proactive approach. This may sound daunting, but modern tools let you automate many security tasks and support your human security experts with capable AI. This doesn't just improve your security posture. It can also reduce insurance premiums, make compliance reporting easier, and help you make full use of network resources.

Highlights include:

- Understand the difference between proactive and reactive security measures
- Discover the business benefits of being proactive
- Learn how to advance both your bottom line and your information security

Table of Contents

Being Proactive Vs. Reactive	3
The Business Benefits of Being Proactive.....	5
Advancing Both Your Bottom Line and Your Information Security.....	5

Cybersecurity is asymmetric warfare taken to an extreme. As the adage goes, cybercriminals only have to get it right once; you have to get it right 100% of the time. Successful attacks require significantly fewer resources than the reciprocal defense. Facing highly motivated and well-equipped threat actors requires a proactive approach. Cybersecurity leaders must build a security program predicated on predicted attacks, with the ability to rapidly pivot defenses to emerging threats. So, how do we do that today?

Understanding your threat landscape and profile becomes the foundation of your program. You face industrialized criminal adversaries that develop modular and malleable malware, share resources across a well-established dark economy, and contract experts at all stages of an attack. Like Fortune 500 companies, these groups employ specialists, and use agile development methodologies, and even leverage shell companies to trick security vendors into technical demos and sharing specifications. This DevOps-like approach to cybercrime allows threat actors to evolve rapidly with an asymmetrical advantage over their targets.



This DevOps-like approach to cybercrime allows threat actors to evolve rapidly with an asymmetrical advantage over their targets.

Threat intelligence and vulnerability assessments help define your risk. Understanding your adversary and their metagame is the first step. Looking for suspicious activity requires the ability to collect telemetry and data, aggregate this enormous volume of data with threat intelligence, and then analyze the data in real time. Machine learning is critical to collecting, aggregating, and filtering data to expose Indicators of Compromise (IoCs).

Human experts are critical in the security equation. Demand for experts and an ever-changing threat landscape means this finite talent pool is challenging to recruit, far harder to retain, and difficult to continuously train-up. The talent pool at any given time is fixed, has not remotely met demand for well over a decade, and training replacement talent takes years.

Your threat surface is both geographically and virtually distributed and, often, poorly mapped Hybrid environments include protected assets, critical business systems that traverse cloud infrastructure (IaaS), cloud applications (SaaS), and remote devices. Few companies have the resources and expertise to properly secure this nebulous mix of services.



Your threat surface is both geographically and virtually distributed and, often, poorly mapped.

Therefore, you need security products and services that remove the burden from your staff. These services must automatically scan for misconfigurations, malfunctions, compliance violations, and other IoCs. They need to automate tasks like writing rules to identify behaviors out of band from a baseline, providing real-time forensics to security operations analysts, and live, auto-generated compliance reports. Security products and services must be quick to deploy, low in resource consumption, and scalable to adapt to new threats and emerging technology.

Security products must constantly monitor the environment for signs of intrusion. Good security products go beyond simple alerting, and provide automated rules, policy updates, and mitigation actions to optimize your security and network control points. Rapid detection and response means threats are contained before they become business disrupting. A simple example is notification and automatic account resets for compromised credentials.

A proactive security approach offers business benefits—both in terms of fewer costly security incidents, and overall efficiency optimizations. The same investments invisibility, observability, and automation which benefit security also help provide accurate information about resource utilization. This leads to less downtime in day-to-day IT operations, as well as better resilience and responsiveness to change.

Being Proactive vs. Being Reactive

Despite your IT security team's best efforts, it's very likely your organization will be compromised. This unfortunate reality of our heavily digitized world is even now recognized by [St. Mary's Journal on Legal Malpractice & Ethics](#), which states "a failure to find adequate funds for cybersecurity improvements will make law firms more vulnerable to cyberattacks, but it also makes it difficult for them to comply with professional responsibility norms, thus resulting in greater legal malpractice and other risks."



A proactive security approach offers business benefits both in terms of fewer costly security incidents, and overall efficiency optimizations.

"Depending on what survey you read, anywhere from **37%** to **80%** of respondents have been hit by ransomware in the past year; around **60%** is the most commonly reported figure. This relates to ransomware alone, not other kinds of cyberattacks, data breaches, or fraudulent wire transfers (FTF).

In the face of such odds, many business leaders adopt a fatalistic approach. They surrender to unstoppable threat actors, and put too much faith

in their backup systems and cyber insurance coverage to weather the storm. This absolutist perspective can lead to reluctance to invest in information security tools, personnel, or alterations to business processes because they cannot be guaranteed to completely resolve the issue. As the adage goes, there are never enough resources to do it right, but there are always resources to do it over.

This perspective commonly manifests in a bias toward minimum security requirements, skewed to investment in backup systems, disaster recovery services, and an incident response retainer. The fallacy and consequence of this mindset is expensive security breaches, lost productivity and revenue, costly penalties and clean-up costs, and irreparable reputational harm.

However, insurance companies are starting to notice the negative consequences of customers taking this approach. The majority of cyber insurance policies with claims lost money for the underwriter. **In response**, insurance companies are increasing premiums, reducing coverage, and tightening minimum policyholder security standards to break the claim-first response to security attacks.

If you want reasonable insurance premiums, your organization would do well to adopt a more proactive approach to detection and response. This has multiple potential benefits. Faster response means fewer security incidents. Fewer incidents or breaches greatly lowers operational costs and protects your business from intangible damage.

So, what do you need to do to get proactive about security? A good start is to address your organization's ongoing technical debt by retiring obsolete or unsecure IT systems. These systems require significant patching, and are often no longer supported by their vendors. Criminals use these vulnerabilities as well-known exploit vectors. Streamlining IT infrastructure reduces

your overall threat profile and means you can focus monitoring and response on the most important systems. It also focuses planning and training, with more effective incident response drills, so that everyone knows what to do when compromise events do occur.



As the adage goes, there are never enough resources to do it right, but there are always resources to do it over.

This may sound like vague advice. What most people want is a simple checklist full of things to do that will guarantee that their network is as secure as possible. Unfortunately, checklist security **has been proven** to be a dangerous and unhelpful approach to security. Every network is unique, and as such each network needs to be audited by trained security professionals whose recommendations are then put into practice.

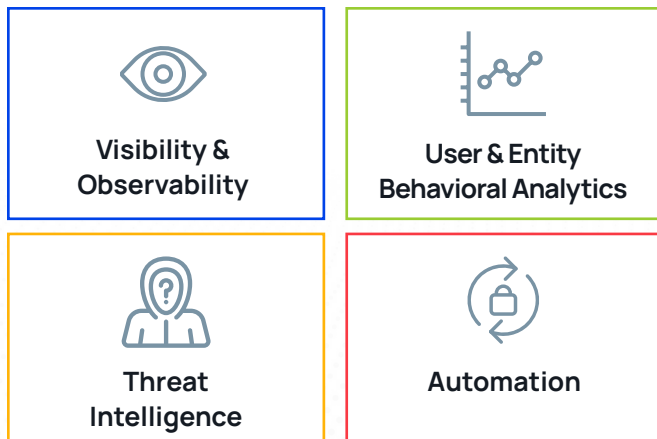


Figure 1: The four aspects of modern information security

There are four aspects of modern information security to be aware of, as they are critical to defending a modern network, as shown in Figure 1.

Visibility & Observability are the foundation upon which all other security efforts are built. Visibility and observability involve a broad range of technologies from monitoring (such as log analysis or real-time telemetry) to data visualization and dashboarding. It means collecting data on what various systems are doing, and then representing that in a way that both humans and computers can understand.

You cannot defend yourself against threats you can't see. Nor can you determine what approaches or controls are not working as intended, which robs you of the ability to baseline and establish what is "normal" as a means of quickly identifying what is not and is likely malicious.

User & Entity Behavioral Analytics (UEBA) are technologies that process data from visibility and observability technologies to establish "normal." Whenever they detect something abnormal, these analytics tools attempt to classify the abnormal behavior, provide contextual forensics, and offer recommended containment and mitigation actions.

Threat Intelligence is a service provided by security vendors that helps information security professionals keep up to date on what known threat actors are up to. This means that, for example, user and entity behavior analytics applications can look at patterns of abnormal behavior and then determine that this matches attacks from a specific threat actor. The threat actor is known to use specific tools and techniques, so information security professionals can then do a deep scan of their network to look for evidence of those tools and/or configuration changes, to see if compromises may have occurred.

Automation, when done right, brings the concept of intent to IT operations. This means that what you expect your IT to do is codified somewhere, such as in YAML files, and this intent is then applied to your infrastructure via an automation engine. Intent-based automation optimizes the process of

determining normal operation within your network: Normal is neatly codified in your intent system, and any configuration that deviates from that codified intent is a problem. In addition, automation can be used to recover from compromise events. Once a problem is identified, automation can help quarantine or shut down compromised systems. Automation can also offer secure alternative replacement systems in place of those that were compromised, reducing downtime. Put simply, visibility and observability tell you what is happening on your network. UEBA lets you know if something on your network is behaving in an unexpected fashion. Threat intelligence can tell you how concerned you need to be about that behavior, while automation can help you deal with the problem quickly and efficiently.

The Business Benefits of Being Proactive

IT administration is challenging for practitioners. Information security is especially complicated. Succeeding at either security or day-to-day operations requires software that takes as much of the load off IT staff as possible. The lower your staff's day-to-day burden, the larger the technology estate that you can manage with the same number of people, and with greater responsiveness to change.

Software that helps ease your IT burden starts with software that's capable of monitoring all the things, alongside analytics and machine learning, which helps your staff prioritize alerts and containment actions. While visibility and observability are often viewed solely

as investments in information security, they're also investments in your organization's operational efficiency.

Consider, for example, asset management. You can't defend what you don't know you have, making asset management the start of a concerted information security effort. But asset management is also useful elsewhere: Once you know what you have, you can start automating your IT.

In addition, asset management is helpful to your accounting team. It allows them to automatically track assets, making it easier to handle depreciation for tax purposes. Asset management can also reduce the time spent on external audits from months to days, and it provides your IT teams the foundation they need to begin automating your organization's IT infrastructure.

Advancing Both Your Bottom Line and Your Information Security

Asset management is only one example of how investing in information security is an investment in IT operations. A well-characterized (and well-monitored) network is just easier to work with.

When something breaks in a well-characterized network the impact of that system failure is easy to understand. Identifying the root cause takes a small fraction of the time it otherwise would. Similarly, a compromise is easier to spot if you know what "normal" looks like, making it easier to catch compromise events at an early stage before attackers have a chance to move laterally and compromise additional systems within your network.



Streamlining IT infrastructure reduces your overall threat profile and means you can focus monitoring and response on the most important systems.

In addition, well-characterized networks are also extremely helpful in terms of business planning. Supply chain issues look set to persist for an unknown number of years, so the ability to fully understand your existing resource utilization can save you from over-investing. Similarly, having a handle on your resource utilization allows you to plan for growth as far in advance as possible, and with a high degree of accuracy.

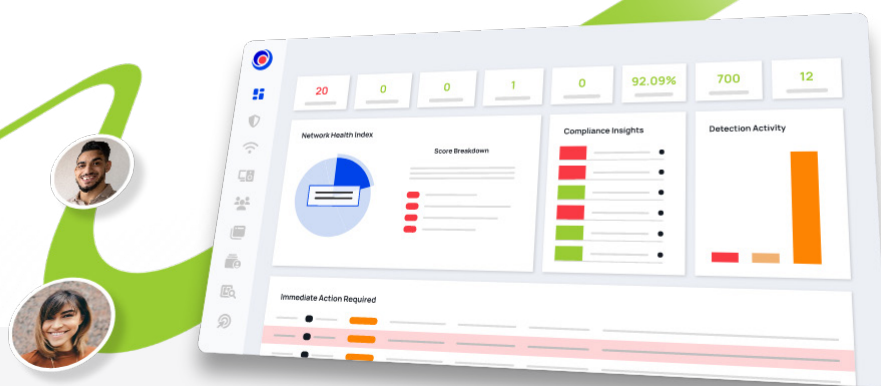
Well-characterized networks are also the easiest to pivot. If you must make substantial changes to your

network for any reason, knowing what you have, where it is, and how it's being used significantly reduces the planning efforts (and possibly financial investment) required of a pivot.

Investing in information security is investing in the efficiency of your organization. Technologies providing the ability to return your operations to “normal” after a compromise event are the same technologies that make recovering from equipment failure or responding to change simple and fast.



The lower your staff’s day-to-day burden, the larger the technology estate that you can manage with the same number of people, and with greater responsiveness to change.



About Adlumin

What you can't see poses the greatest risk to your organization. Your exposures lurk in the cloud, hybrid environments, and the darknet. There are countless gaps where threats can hide before they lead to business disrupting events like ransomware shutdowns or massive data breaches.

Adlumin Inc. is a patented, cloud-native Managed Detection and Response (MDR) and services platform. The platform focuses on advanced cyber threats, system vulnerabilities, and sprawling IT operations to command greater visibility, stop threats, reduce your business risk, and automate compliance. As the command center for security operations, Adlumin leverages powerful machine learning, identifies critical threats, automates remediation rules and systems updates, and provides live continuous compliance reporting. Don't let your organization get caught in the dark.

Illuminate Threats, Eliminate Risks, and Command Authority with Adlumin. www.adlumin.com