PERSISTENT AUTHENTICATION. **ALWAYS ON GUARD.**

3 Proven Strategies to Outsmart Modern Cybercriminals

PROXIMIA®

Table of Contents

Staying Ahead of Cybercriminals: It's Time For Security to Catch Up

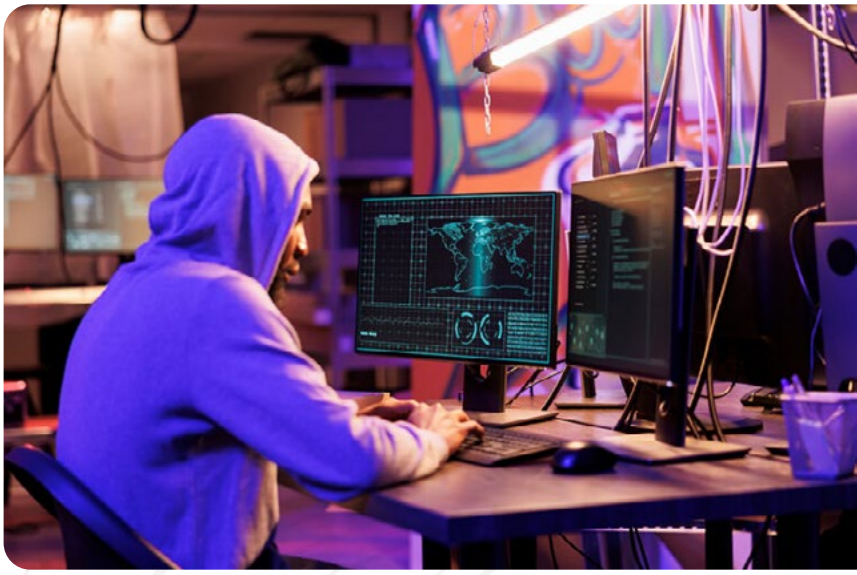
Businesses have their backs against the wall as cybersecurity threats increase in frequency and severity. Proximia believes it's time for security teams to be as imaginative and innovative as threat actors have become. Not just new approaches to fundamentals but evaluating new kinds of defenses and controls as well. As risk slows the business down, security must move faster.

How did we get here?

To add protection, many turn to MFA, often using bioauthenticators like Face ID. While MFA restricts unauthorized access initially, it doesn't secure the entire session. Additionally, current MFA methods can be cumbersome and time-consuming, leaving users frustrated and less likely to embrace these security measures.

In the outside world, it's easier to get good at being bad

If you've seen more than one heist movie, you know how much work goes into the setup. First, recruit the right professionals. Then it's on to selecting a target and finally all those classic stakeout and surveillance scenes. And all this takes place before the job even goes off.



Say what you want about those movie bad guys – their work ethic was typically impeccable.

While it's true that criminals have never been as smart or determined as they are in the movies--they don't have to be. The same digital changes transforming how we live and work have made it very easy for a single bad actor to have the same diverse capabilities of a well-curated Hollywood heist crew.

They're getting smarter

With all the information they can get by browsing, buying, or stealing, threat actors can quickly understand your business and identify your most valuable resource(s). For ransomware attacks, again the leading attack type, the real prize isn't data, but your ability to do business. It's like the heist crew stealing the bank itself.

Finally, They're also getting smarter about their business model. Large ransom operations even run call centers to speed the payment of demands. Some attacks are made with full knowledge of cyber insurance limits in order to drive faster payouts. It's hard not to be a little impressed.

Technology lets them do more with less

The huge financial incentives in cybercrime drive a culture of continuous innovation that most businesses would envy. This advancement enables attackers to combine and converge individual threats, tactics, and procedures into complex, multiphase threats.

This also includes threat actors using AI and GenAI to become more effective. From supercharged tactics such as automated port scanning to sophisticated Gen AI deep fakes, cybercriminals are using AI to stay ahead of your defenses. It all comes together in crime as a service, where cybercriminals offer their services to others. This creates a very dangerous marketplace where even relatively inexperienced threat actors can easily assemble an all-star crew.

Businesses Are Moving Fast But Still Falling Behind

While criminals are getting smarter and more effective, too many businesses are going in the other direction. It's probably a combination of wishful thinking and sustained weariness, but it's putting a lot at risk.

Size and industry are no longer a defense

While the headlines are filled with stories about the cybersecurity failures of large, well-known companies, threat actors are always looking far and wide for their next target. As large companies get more sophisticated about the way they protect critical assets, it's only natural that threat actors seek smaller, easier prey.

The move to a software-defined enterprise also makes smaller businesses more attractive. In many cases they're using the same applications and infrastructure as larger organizations, but without the same security maturity. Even moving to a public cloud still leaves much of the challenge in the laps of internal IT and security teams.

Data is a big asset, but a bigger liability

From sales operations and finance through to customer service, chances are you rely on data to either drive your business, or at least make it run faster and further. You're probably also collecting as much customer data as you can ethically get your hands on, while trying to stay compliant with the tougher and tougher rules where you operate.

Threat actors have also noticed you're increasing reliance on data, thus the rise of ransomware. But it's also great for just adding to the stress and strain of IT and security teams. In fact, compliance rules, many data-driven, put an average 4,300 hours of work on the plates of IT and security teams at growing businesses.

Finally, third party risk is multiplying your obligations

Modern business relationships are increasing your attack surface just as regulators are becoming intensely focused on third party risk. You're now accountable for the security posture of partners. And you don't have to fall under security rules directly—business agreements will inevitably bring these rules your way.

The complexity of the software-defined business also makes this worse. Larger orgs have an average SaaS portfolio of 371 applications and services. Understanding and assessing 3rd party readiness, and being able to attest to your own, demands consistent standards for measuring and benchmarking. Those standards remain as big a barrier as any killer security app.

There Is Good News, We Promise

If you stare long enough at cybersecurity headlines, it's easy to quickly get very discouraged –the hits just keep coming. Even as cybersecurity defenses get stronger, attackers manage to remain forever just out of reach. Businesses are struggling to acquire both talent and tech. In an era where everything is automated, so is the dread about the next incident or actual breach.

But if you're a regular reader of one of the cybersecurity industry's big yearly reports, you know there is room for optimism. The IBM Ponemon 2024 "Cost of a Data Breach Report" shows some very important numbers moving the right way.

- **Attackers are being detected earlier, limiting damage and speeding remediation:** This year's report said the average breach was detected in 50 days, down from 59 from last year. That's still a long time, but it's progress.
- **Attackers are more frequently being detected by internal security teams and tools:** The 2024 report shows 42% of breaches being detected by internal teams, up almost 10% over the previous year. This demonstrated that businesses are getting more serious about threat detection.

Taken together, the two stats show some real evidence of increased effectiveness—we know the cybercriminals certainly haven't slowed down. So where teams are being more successful, what's happening?

How it's getting better: rethinking basics, reframing fundamentals

Security tools are getting smarter, but the shift in mindset iseven more significant. Security in motion must be about orchestration beyond implementation. The same point solutions that once sat in a stack must become part of a connected whole that understands more and can respond more effectively.

3 Proven Strategies to Outsmart Modern Cybercriminals

1. Think in Layers, Not Single Checkpoints

The rise of zero trust has come from the failure of today's outdated paradigms: no single defense is sufficient, and you can't rely on catching the bad guys on their way in. Rather than relying solely on perimeter defenses, cybersecurity requires a layered approach that builds in multiple, adaptable barriers. Multi-factor authentication (MFA), for example, isn't a standalone solution; it's part of a broader framework where each layer adjusts to provide protection in proportion to the level of risk. Over time, this layered approach leads to stronger defenses, enhancing the security of data, identities, applications, and other digital assets.

2. Unlock Intelligence Through Convergence

The future of security lies in connecting information from diverse security tools to form a comprehensive defense. Point solutions alone lack the capacity to respond to complex attacks effectively. By integrating these tools into a unified system, they collectively learn and share insights, using AI to enhance real-time analysis and incident response. Convergence transforms individual security tools into a network that adapts to emerging threats, where each component informs and strengthens the whole.

3. Build Resilience with Adaptive Threat Detection

Cybersecurity success increasingly hinges on rapid learning and adaptation. Today's threats evolve constantly, making it essential to anticipate changes in attack methods. Adaptive threat detection involves a proactive mindset that quickly assimilates new information, responds dynamically to emerging risks, and uses behavioral analytics to identify irregular patterns. By staying agile and continuously adjusting to both internal and external shifts, businesses can better position themselves to meet the future of cybersecurity head-on.

Complexity isn't going anywhere, but confidence is still possible

The continued gloom and doom around risk and cybersecurity is inevitable and understandable. For all our spending and innovation, the numbers always seem to move in the wrong direction. So where does the pivot begin? How can you be prepared for when the next heist crew, no matter how big or experienced, comes calling?

Proximia knows your best chance at cybersecurity success lies in giving your security experts the power of modern solutions – and the ability to craft new strategies around them. This is how traditional controls and point defenses take on new effectiveness, while the best of what's next becomes part of the next generation of security and risk best practices.

888.795.1480 | proximia.com