DEFENSESTORM
THE BEST OFFENSE.

EBOOK



DETECTION IS THE CONTROL THAT MATTERS NOW

AI collapsed the time from vulnerability disclosure to exploitation. Here's what still works, and where banks and credit unions should invest next.

FOR BANKS & CREDIT UNIONS

Built for banking.

01

THE NEW ECONOMICS OF EXPLOITATION

Cyberattack techniques rarely sit still, but the past year's shift should concern every security leader. AI has rewritten the economics of vulnerability exploitation.

A multi-agent LLM framework called **CVE-Genie** reproduced more than half of recently published CVEs with verified, functional exploits, in minutes, for roughly the price of a coffee. The attacker's toolkit got dramatically cheaper, faster, and more automated in a very short window.

AND THE MARKET IS SCALING

AI tools advertised on ransomware forums jumped from **38 posts in December 2025 to 1,486 in February 2026.**

51% of CVEs published June 2024–May 2025 reproduced with verified, functional exploits

18 min median time to a working exploit

$2.77 average cost per exploit generated

Source: CVE-Genie (arXiv, 2025)

02

THE PATCH WINDOW HAS CLOSED

Most security programs were built on an assumption that no longer holds: that there would be enough time between a vulnerability being disclosed and it being exploited to close the gap with a patch or a control.

That window has collapsed. A vulnerability-management program running on **weekly or monthly patch cycles is now structurally mismatched** to a timeline measured in hours.

700 → **44**

median days from disclosure to exploitation, 2020 vs. 2025

28.3%

of CVEs are now exploited within **24 hours** of public disclosure

Source: VulnCheck, Q1 2025

03

WHY TRADITIONAL CONTROLS FALL SHORT

Preventive controls still matter. Firewalls, segmentation, patch management, and vulnerability scanning are not obsolete. But signature-based detection can only match patterns it already knows, and **a zero-day has no known signature yet.** AI-assisted exploitation makes that limitation easy to abuse at scale and very low cost.



THE PERIMETER IS THE TARGET

Edge devices (firewalls, VPNs, routers) carry privileged access with limited monitoring behind them. The Check Point VPN zero-day, the sixth actively exploited Cisco vulnerability of 2026, and multiple Palo Alto firewall flaws all follow the same pattern: the tools built to protect the perimeter have become the way in.

56% of vulnerabilities tracked in 2025 required **zero authentication** to exploit

40% of incidents came from vulnerability exploitation, the leading cause of attack in 2025

Source: IBM 2026 X-Force Threat Index

> The industry over-invested in controls that assume a stable perimeter, and under-invested in the capability to detect and respond when it fails.
>
> **Rick Howard**
> Cybersecurity First Principles (paraphrased)

04

WHAT ACTUALLY WORKS

If signature-based controls can't stop what they haven't seen, and patching can't keep pace with an exploitation timeline measured in hours, then **detection is the control that actually matters.** The institutions that stay protected over the next few years are the ones investing in behavioral detection and around-the-clock coverage.

BEHAVIORAL EDR

Endpoint detection and response flags suspicious activity by behavior rather than signature, which is what makes it effective against attacks with no known fingerprint yet.

AN MDR LAYER

Managed detection and response brings the around-the-clock coverage most community banks and credit unions can't reasonably staff internally.

A COLLABORATIVE SOC

Banking-fluent cybersecurity analysts, available 24/7, who act on what they're seeing, the difference between detecting a compromise in progress and discovering it after the fact.

Detection is the control that matters now.

05

WHERE TO FOCUS NOW

Start with measurement. The gaps in your answers point directly to where the investment needs to go.
The goal is heuristic detection at speed, across your entire infrastructure.

1. What is your mean time to detection across the kill chain?
2. What percentage of monitoring runs around the clock versus business hours only?
3. How much of your detection capability is behavioral versus signature-based?
4. How strong is your detection coverage across your entire infrastructure?



THE RISK IS GROWING DAILY

The exploitation timeline has compressed to hours. Banks and credit unions without 24/7 detection coverage are carrying a risk that grows by the day.

06

KEY TAKEAWAYS

AI rewrote the economics

Working exploits now take minutes and cost dollars, automated, at scale.

The patch window is gone

Nearly 1 in 3 CVEs is exploited within 24 hours; weekly cycles can't keep up.

Signatures can't see zero-days

And 56% of 2025 vulnerabilities needed no authentication at all.

The perimeter is the target

Edge devices are now preferred entry points, with little monitoring behind them.

Detection is the control

Behavioral EDR, an MDR layer, and a 24/7 Collaborative SOC that acts on what it sees.

Measure to prioritize

MTTD across the kill chain, % 24/7 coverage, and % behavioral vs. signature.

07

THE GAP BETWEEN KNOWING AND DOING

The conclusion is the same one a thorough assessment would reach on its own: you need behavioral detection, a managed layer that runs around the clock, and analysts who act on what they see. Knowing that is not the hard part. Running it is. Most community banks and credit unions cannot hire, tune, and staff 24/7 behavioral detection on their own, and the ones that try often end up with tools no one has the time to watch.

That gap is what DefenseStorm was built to close, for banks and credit unions specifically. Not a generalist security vendor with a banking brochure, but detection, response, and examiner-ready evidence built for how financial institutions actually operate.



THE POINT OF DETECTION IS SPEED

A control only matters if it catches a compromise in progress. Our Collaborative SOC works from a mean time to detection typically under three minutes, measured from the moment data reaches us to a tracked investigation.

08

BUILT FOR BANKING, NOT BOLTED ON

DefenseStorm is the only cyber risk platform built exclusively for U.S. banks and credit unions. Detection, response, and governance run in one system, backed by a U.S.-based Collaborative SOC of banking-fluent cybersecurity analysts who act as an extension of your team.

THE ENGINE

GRID Active

Our intelligent data engine ingests roughly 80 million events a day per institution and filters the noise down to about three that need a person, a 99.9% reduction, so nothing real gets buried.

THE PEOPLE

24/7 Collaborative SOC

Banking-fluent cybersecurity analysts on watch around the clock, with detection typically under three minutes and client notification under twenty, under eight for critical cases.

THE DETECTION

Tuned to Banking

More than 750 detection triggers written for financial workflows, catching over 98% of tested attacks, behavioral by design so novel threats do not slip past a missing signature.

THE EVIDENCE

Examiner-Aligned

Detection generates audit-ready evidence as it happens, mapped across 16,000+ banking controls, producing thousands of artifacts a year and roughly 70% less exam prep.

09

WHERE DEFENSESTORM CLOSES THE GAP

Each of these shifts has a direct answer in how DefenseStorm runs detection for banks and credit unions.

THE PATCH WINDOW HAS CLOSED

Behavioral detection that does not wait for a signature or a patch, catching over 98% of tested attacks by how they act rather than what they match.

THREATS DO NOT KEEP BUSINESS HOURS

A 24/7 Collaborative SOC with detection typically under three minutes and client notification under twenty, so a compromise is caught in progress, not after.

THE PERIMETER IS THE TARGET

Coverage across your full infrastructure, roughly 80 million events a day filtered to the few that need a person, so edge activity is not a blind spot.

YOU CANNOT IMPROVE WHAT YOU CANNOT MEASURE

Continuous visibility into detection speed and coverage, plus thousands of audit-ready artifacts a year that prove it to your examiner.

DEFENSESTORM
THE BEST OFFENSE.

YOUR NEXT STEP

SEE WHAT 24/7 DETECTION LOOKS LIKE FOR YOUR FI

DefenseStorm pairs behavioral detection with a 24/7 Collaborative SOC built exclusively for banks and credit unions, so a compromise gets caught in progress, not discovered after the fact. Book a demo and we'll walk through your detection coverage together.

REQUEST A DEMO →

DefenseStorm

The only cyber risk platform built exclusively for U.S. banks and credit unions, bringing MDR, risk, and governance into one system. The GRID Active Platform is backed by a U.S.-based 24/7 Collaborative SOC of banking-fluent cybersecurity analysts who act as an extension of your team.

1725 Windward Concourse, Suite 425, Alpharetta, GA 30005 · 470-519-0020 · info@defensestorm.com · www.defensestorm.com

SOURCES

CVE-Genie (arXiv 2509.01835); Halcyon via CSO Online; VulnCheck Q1 2025 via The Hacker News; Flashpoint n-day trends; IBM 2026 X-Force Threat Index; Rapid7 (Check Point CVE-2026-50751); SecurityWeek (Cisco SD-WAN zero-days); Rick Howard, Cybersecurity First Principles.

© 2026 DefenseStorm. All rights reserved.

Built for banking.