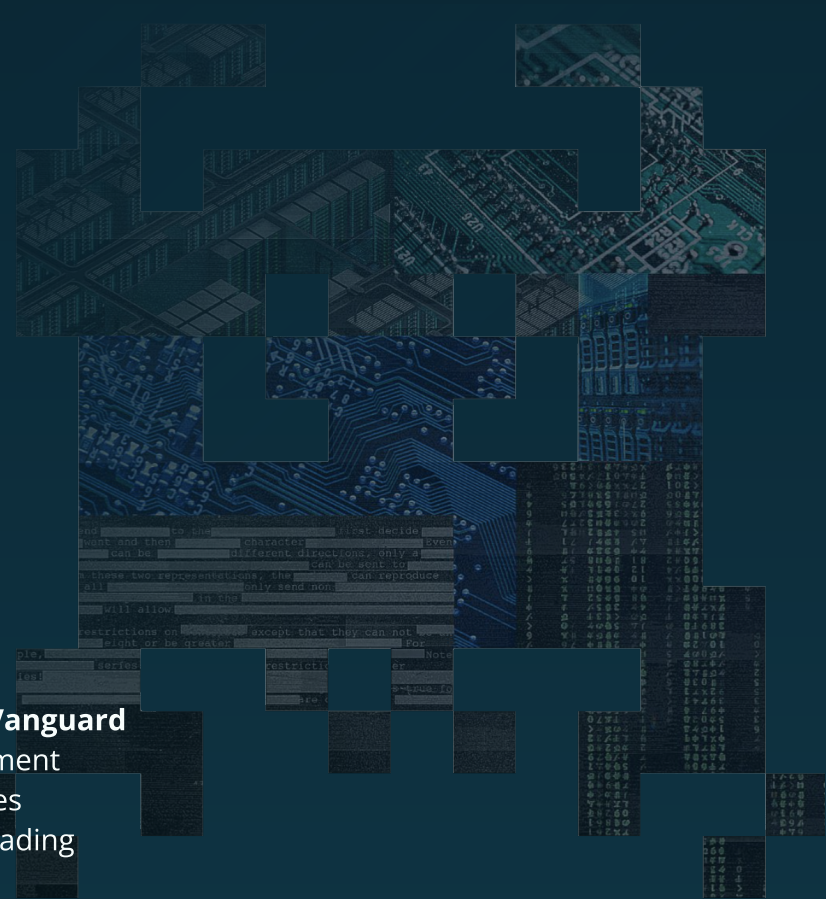


Intruder Vanguard

Continuous and comprehensive penetration testing.
Find what scanners can't.



A selection of customer stories from our **Vanguard** solution — a hybrid vulnerability management solution uncovering high-risk vulnerabilities continuously led by some of the world's leading security professionals.

Great coverage, leading expertise, intelligence-driven investigations

Our security professionals closely monitor vulnerability disclosures across various feeds and news sources. As new severe vulnerabilities arise, the Intruder team's first thoughts are:

"How does this affect our **Vanguard** clients?"

Most vulnerability scanning engines will detect **Log4Shell** (CVE-2021-44228), and many have been running checks for it since the day it was discovered. However, because vulnerability scanners operate across a range of organisations and tech stacks, the checks can be quite generic in nature. From the moment we saw the vulnerability, our Vanguard customers received additional scrutiny from our team of expert hackers, who used more tailored techniques, including WAF bypasses. This meant we were able to find vulnerable systems where a standard vulnerability scan could not.

A recent critical Microsoft Exchange vulnerability, nicknamed **Proxylogon**, provides another good example. Having heard reports of the vulnerability from Microsoft and the security community, Intruder immediately implemented its own proof of concept code to scan its Vanguard clients, all before the other market-leading vulnerability scanners added checks. This rapid response was vital, as state-sponsored threat actors were already working to exploit the vulnerability.

One of our clients, a major automotive manufacturer, was affected by Proxylogon, and after thorough testing, Intruder gained complete control over a vulnerable Exchange server. Instant notifications from the Intruder Vanguard team meant our client could patch and re-test its system to ensure the vulnerability was no longer exploitable.

This critical response led to the Intruder team promptly running tests across other Vanguard clients' Exchange servers for the same exposure. Our expert professionals were able to probe deeper, and their expertise and technical analysis allowed them to conclude that not a single other system was vulnerable.

All clients received a timely "all clear" confirmation, reassuring them that they were covered and their teams could focus on other critical areas of remediation.

“

Thanks guys, this was super helpful. We are now patched and protected 😊

Endpoint protection software provider

”



Vanguard clients have received early warning of similar Microsoft Exchange weaknesses, such as the high severity **Forgot2kEyXCHANGE**. Intruder's Vanguard team tracked this disclosure from its first announcement as part of Microsoft's Patch Tuesday, and quickly identified 20 vulnerable systems across three Vanguard customers. All were immediately notified and took appropriate action.

SMBGhost is another severe and potentially wormable vulnerability affecting Windows systems. An Emerging Threat Scan from Intruder identified SMBGhost on a Vanguard client, and through active investigation of the public exploits for the vulnerability, we concluded that they were not fully functioning. The client received immediate communication from our Vanguard experts that although public exploits had not successfully exploited their configuration, our advice was to restrict access to the target further. There are always modified undisclosed exploits which cannot be reasonably tested and it might only be a matter of hours before more working exploits are publicly released that target a wider range of configurations.

“

The **Vanguard** add-on really takes the product to the next level. Having security engineers who are familiar with our site look at the automated results and verify them is definitely worth it. With Vanguard, they can also proactively look for more complex issues like a hacker would. Intruder found a critical issue in their first month that was worth the whole cost of the product.

Jason, Analytics Engineer at Worthpoint

”

Though lacking a catchy name, **CVE-2020-3452** was a similar case. This flaw offers attackers the ability to download arbitrary files from vulnerable Cisco networking devices. After the vulnerability hit the news, the team identified its presence on systems belonging to two Vanguard clients. Exploitation, however, did not uncover any overly sensitive files.

Security oversight, issue detection, and remediation speed

The signal to noise ratio from vulnerability scanning isn't always perfect, and an extra set of eyes to review scan results is highly beneficial. False positive elimination is a popular feature of the **Vanguard** solution — where manual vulnerability checks remove findings that are not exploitable.

In some cases, automated vulnerability scanners can incorrectly represent legitimate threats and their business impact. This is due to their generic fit-every-use-case nature. But with Intruder's hybrid scanning and security team solution, Vanguard, businesses gain an additional layer on business risk and context to give them an accurate, data-driven representation of their current state.



For example, after reviewing a client's monthly scan, Intruder's analysts noted that the automated scanner had flagged an issue that the company didn't believe. Our Vanguard team was able to have the issue contextualised by demonstrating that the weakness was, in fact, exploitable with the ability to gain direct access to a database system. In addition, the database housed sensitive personal information of site users, the leakage of which could have posed regulatory ramifications. As a result, the client prioritised internally for remediation.

Another case where the severity levels assigned by vulnerability scanners don't always reflect the actual risk presented by security weaknesses is when an administrative panel exposed to the internet is a low or medium risk. For example, perhaps the admin uses weak credentials to login, which an attacker can easily guess. This was the case for one Vanguard client, and it meant that IP-camera footage from inside an industrial warehouse was in effect openly accessible to the internet. As a result, the severity of the issue in the client's scan results increased to reflect the ease of exploitation and the client was notified.



Comprehensive vulnerability management that works as an extension of your security team

It's no secret that automation offers IT security divisions a major edge. Overstretched teams need tools that lighten the workload so that they can take a more proactive approach to security and place greater focus on business critical tasks.

Intruder Vanguard goes way beyond automated vulnerability scanning by supporting users with manual reviews carried out by dedicated security experts, comparable to a continuous penetration test. Equipped to spot more sophisticated weaknesses, they provide advisories with actionable instructions, so technical teams can remediate critical issues faster.

For a large infrastructure enterprise such as Hill & Smith Holdings PLC, this impact was key, enabling it to achieve expanded threat coverage and understand the direct impact on the business. Sam Ainscow, Group CISO for Hill & Smith said, "The Vanguard solution will find things that automated scanning doesn't. Every time Vanguard's professional security team finds something, it delivers value."

Intruder Vanguard goes further, seeking out additional assets that may be in use to provide a full picture of the vulnerabilities that exist. In addition, the service helps in reducing the number of false positives and in identifying potential disasters where different vulnerabilities might combine to result in far more severe outcomes.

Switching to Intruder Vanguard transformed the way Hill & Smith handled infrastructure security weaknesses for the better. With a team of dedicated security experts constantly hunting for dangerous vulnerabilities, Intruder Vanguard fills the gap that exists with point-in-time penetration tests, and provides Hill & Smith with a strong overview and protection of its systems. Problems are uncovered and advisories are raised within hours, ultimately letting them implement fixes within days.

“

Maybe one percent of businesses already have everything they need in-house. Intruder **Vanguard** is for the other 99 percent, the ones that need to augment teams with on-demand security talent and empower decision-makers with a real-world understanding of the risks associated with their external attack surfaces at any given moment.

Sam, Group CISO at Hill & Smith

”

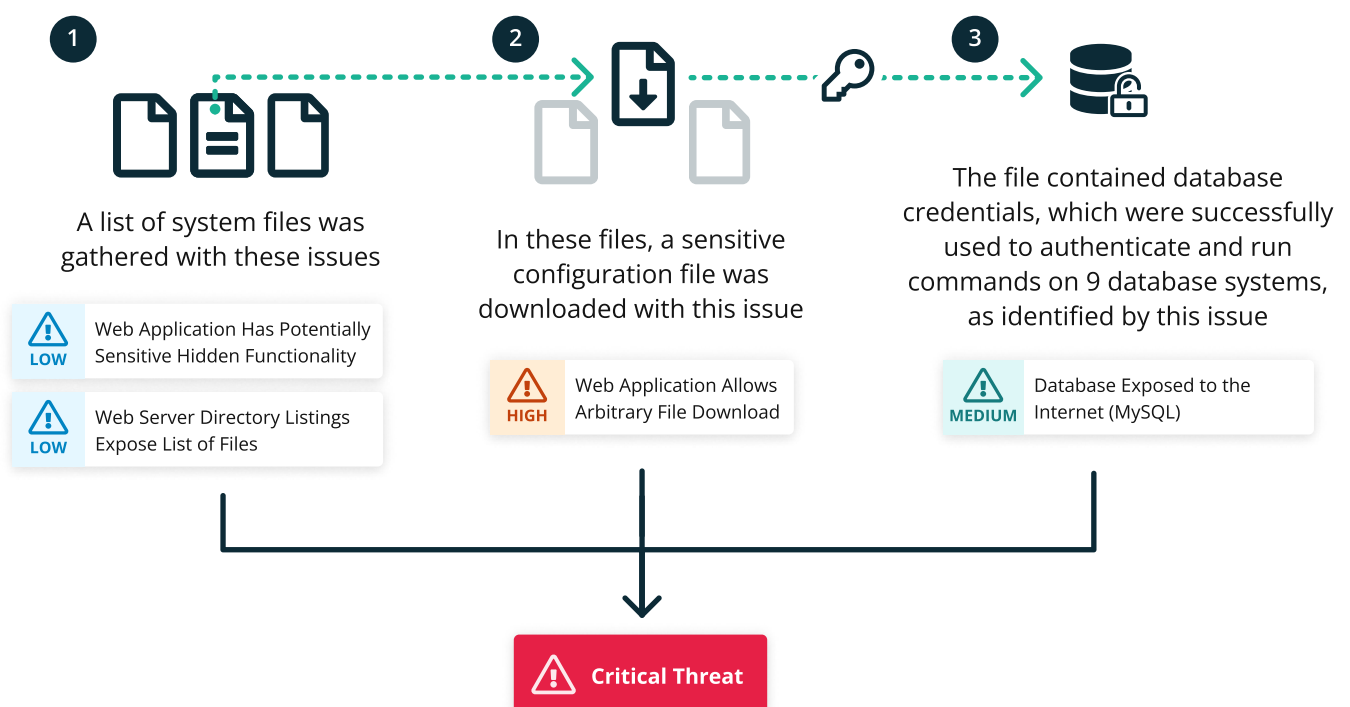
Chained exploitation solved with accurate, contextual-driven guidance

Intruder's penetration testers are encouraged to proactively seek out weaknesses within the assets under the protection of **Vanguard**. These highly skilled testers have a knack for discerning small vulnerabilities in scan reports which in combination are greater than the sum of their parts.

For a large enterprise in the eCommerce sector, the Vanguard team was able to fill the gap between automated scanning and point in time penetration testing, by combining four issues that were reported by our vulnerability scanner.

Our security professionals are positioned to understand your unique environment. They will help you uncover unknown IT assets, analyse scan results, and adjust the severity rating of reported vulnerabilities to reflect the real threat.

In this example, no single finding would be rated a critical severity, however when combined, the threat posed comfortably met that criteria.



Continuous peace of mind

We frequently take requests and out of the ordinary jobs to help clients gain a complete picture of their high-risk vulnerabilities. It's part of our hybrid vulnerability management approach for Intruder **Vanguard**. Here are some examples —

A leading multinational construction company was concerned about the security of some of its **Remote Desktop Services (RDS)**. Our security professionals gave them a thorough review and successfully gained remote access to a domain system.

This system was connected to a wide network, in which an attacker could try to compromise further machines, exfiltrate sensitive information or deploy ransomware.

The client took immediate steps to remediate. When the time came to roll out a new RDS platform, Intruder also assessed this for security weaknesses.

Bug bounty or beg bounty? Gain validation of **bug bounty reports** from third-party security researchers or bounty schemes with Intruder by your side.

The Head of IT Security requested that the **severity of issues** increase to account for internal context and organisation-specific sensitivity. As a result, the team adjusted the issue severities reflected in the client's reporting.

Need a more **customised approach** to scanning? We can deliver ad-hoc scans, scans explicitly targeting a particular weakness, and scan results in specific formats.

Find what scanners can't. Close the gap today.

Intruder's Vanguard solution delivers a hybrid vulnerability management approach in conjunction with manual auditing led by some of the world's leading security professionals.

Our Vanguard professionals are all CREST (CREST Certified Infrastructure, CREST Certified Application) or Offsec certified, adhere to an ethical code of conduct, and have years of penetration testing experience.

BOOK A CALL TODAY

Learn more about how Intruder Vanguard supports security leaders and teams to gain a complete picture of their high-risk vulnerabilities with a hybrid vulnerability management solution.

contact@intruder.io

READ MORE

intruder.io/vanguard



