Secure Your Inbox, Accelerate Compliance:

LevelBlue Email Security with Check Point

LevelBlue | CHECK POINT

The #1 Target for Cyberattacks

Communication and collaboration are the lifeblood of modern businesses. In today's world, the professional relationships that spark innovation and drive success usually involve an array of digital tools and platforms. Among these, email remains the most important. It's no surprise that email is—and long has been—attackers' top target.

Year after year, we continue to see increases in phishing and business email compromise (BEC) threats, and the costs associated with these incidents are growing, too. The increasing complexity of computing environments only adds to the challenge, since businesses are under constant pressure to rapidly adopt new technologies while also maintaining cyber resilience in the face of an ever-more-sophisticated threat landscape.

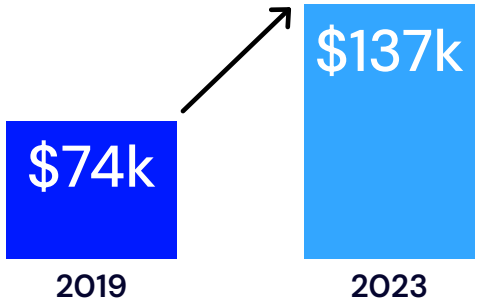
The Costs of Business Email Compromise, According to the FBI

Business email compromise cost 20k+ victims nearly

$3 billion

in 2023.[1]

The average cost of a BEC incident rose.[2]



59%

of the incidents analyzed in the LevelBlue security operations center (SOC) in 2024 stemmed from BEC attacks.

[1]Federal Bureau of Investigation, Internet Crime Complaint Center, Internet Crime Report 2023.
[2]Federal Bureau of Investigation, Public Service Announcement, "Business Email Compromise: The $50 Billion Scam," June 2023.

Regulators Respond to the Threat

In response to a steady stream of high-profile breaches that are devastating for their victims, consumers, and even national security, regulators are stepping up oversight. New rules emphasize transparency and incident disclosure.

- The Securities and Exchange Commission (SEC)'s new **Cybersecurity Risk Management** requirements came into force in late 2023. This regulation mandates that registrants disclose information to investors about any cybersecurity incident deemed to be of "material" importance within 4 business days of its occurrence.[3]
- The **Cyber Incident Reporting for Critical Infrastructure Act** of 2022 requires that covered entities (organizations in critical infrastructure sectors) report cyber incidents to the Critical Infrastructure Security Agency (CISA) within 72 hours of learning that they've taken place. A large number of verticals are considered critical infrastructure, including communications, financial services, and healthcare.[4]
- In Europe—organizations doing business there are also subject to compliance—the **Network and Information Security (NIS) 2.0 directive** will impose far-reaching cyber incident reporting requirements, including the obligation to provide an "early warning" within 24 hours when a significant incident is believed to have occurred.[5]

These rules will increase governments' visibility into the scale and scope of cyberattacks in their countries, providing an opportunity to warn businesses of impending threats that might target them. But they also place a new burden on the organizations who are subject to the regulations, since they must gather the data that will enable prompt reporting, if and when an incident occurs.

The requirements can be particularly challenging for midmarket companies. It can be a struggle to build robust incident readiness and response capabilities with a fraction of the resources that major enterprises have on hand.

For these organizations, building the right workplace security strategy is key.

It's essential to find a solution that:

- safeguards the most common targets—collaboration tools like file sharing, chat, Slack, and Microsoft Teams, as well as email
- is simple to manage
- readies the company to meet audit and reporting requirements

In the rest of this eBook, we'll talk about what this kind of solution looks like, and how you can implement it rapidly and successfully.

[3]U.S. Securities and Exchange Commission, Press Release, "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," July 2023.
[4]CISA, Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).
[5]NIS2 Directive, NIS2 Requirements.

The Never-Ending Battle with Email Attacks

Although organizations have invested in tools, solutions, and processes designed to counter this threat for years, attacks leveraging email (and other collaboration tools) continue to succeed with alarming frequency. And the costs associated with them continue to climb.

Why Is It So Hard to Solve This Problem?

- Email attacks target people, who tend to trust the co-workers, business partners, and friends who communicate with them via this channel. This means it will always be possible to trick them at least some of the time.
- Finding the right email security solution is tricky: the marketplace is crowded, noisy, and rife with exaggerated vendor claims.
- Implementing the solution can be complex. Specialized resources are usually needed for configuration and deployment.
- Email and collaboration ecosystems involve many interoperable products and solutions. The right integrations are important for centralized visibility.
- Regulatory requirements demand logging and reporting capabilities that not all email security solutions can deliver.
- Managing the solution—including 24/7 monitoring—can be resource-intensive, and not all companies have access to the necessary skills in-house.

Building a Robust Email and Collaboration Security Program: What's Needed

There are three elements in any successful security approach: people, process, and technology. To build robust email security capabilities, you'll need the right combination of the three.

In terms of technology, you'll need a solution that can:

Supplement native capabilities

Existing cloud email solutions don't provide defense-in-depth coverage across multiple collaboration platforms. They also may not provide the logging or incident reporting capabilities necessary to keep up with evolving compliance requirements.

Take advantage of AI and advanced technologies

AI is the subject of many conversations right now, but not all solutions that claim to use AI are created equal. AI is a must-have for phishing detection, since it can automatically identify communication patterns and conversation styles that signal malicious intent.

Analyze supply chains and contact chains

AI-driven contact chain analysis enables deep inspection to accurately detect social engineering, executive impersonation, and BEC attacks. Not all solutions offer this capability.

Integrate with the rest of your security stack

This is important for compliance purposes, but also enables full visibility across the entire attack sequence (because ransomware might start with a malicious email, but it doesn't end there). API integrations should enable a broader extended detection and response (XDR) and/or security information and event management (SIEM) or security orchestration, automation and response (SOAR) strategy.

But implementing the right tool isn't enough. You'll also need the resources to deploy, configure, and manage the solution. This is where an MSSP comes into play.

Introducing LevelBlue Email Security with Check Point

Organizations can gain all the capabilities and competencies needed to build a robust email security program by leaning on an industry-leading managed service provider. This will reduce the burden on internal IT teams while delivering superior protection. This approach supports and enables compliance, making you audit-ready and preparing you to meet reporting requirements.

Offered as a fully-managed service, LevelBlue Email Security with Check Point delivers industry-leading protection from socially engineered attacks. The solution helps you:

Block Sophisticated Social Engineering Attacks.

Built-in security controls can't overcome advanced phishing attacks designed to deceive busy or unsuspecting users. With LevelBlue Email Security with Check Point, industry-leading threat intelligence and AI-trained engines thwart attacks before they reach the inbox.

Prevent Infection Via Malicious Attachments.

LevelBlue Email Security with Check Point opens suspicious files or links within a sophisticated, evasion-resistant sandbox to identify never-before-seen (zero day) threats. Proactive threat extraction then removes the malware and returns a safe-file version to the intended user in seconds.

Protect Sensitive Data and Maintain Compliance.

The solution automatically scans subject lines, body content, and attachments to detect when sensitive data is being shared via email or other productivity applications. When detected, sensitive data is immediately blocked or unshared to prevent data leak. You can set predefined or customized policies and rules.

Stop Account Takeover Attacks with Augemented Authentication.

Unauthorized users and compromised devices are prohibited from accessing your cloud email or collaboration applications. LevelBlue Email Security with Check Point transparently augments the identity authentication process, immediately blocking suspicious logins (like multiple location login or bad IP reputation).

Benefits of the LevelBlue approach:

- ✔ Support for a broad array of integrations
- ✔ Expert deployment into your environment
- ✔ 24/7 monitoring and management
- ✔ Logging and retention policies tailored to your organization's individual compliance requirements or internal policies
- ✔ Access to advanced threat protection and AI-driven detection
- ✔ Incident response and recovery support
- ✔ Seamless integration with Microsoft 365, Google Workspace, or other tools you're already using
- ✔ Ongoing training of operational staff

Does my MSSP's email security service ensure continuous, high quality defense against today's evolving threats, while also supporting our organization in maintaining its protection and educating employees?

Questions to ask your MSSP about email security:	Yes	No
Does your solution scan every inbound, outbound, and internal email?		
Can you manage software updates to ensure up-to-date detection of evasive phishing and social engineering attacks?		
Can your solution apply context-aware policies to protect confidential information anywhere in your ecosystem?		
Can you provide training or awareness programs to our staff to mitigate phishing and insider threats?		
Does your solution include 24/7 support with frequent updates to block zero-day malware and ransomware?		
Do you help organizations maintain compliance with regulations like HIPAA and PCI-DSS?		
Does your solution include custom integrations to ensure interoperability across your entire cloud collaboration ecosystem?		

LevelBlue + CheckPoint: Market Leading Email and Collaboration Security Managed by an Award-Winning Team

LevelBlue's expert managed security service team makes it possible to take full advantage of best-in-class solutions such as Check Point Email Security. We serve as a seamless extension of your own security program, providing transparency and visibility into your security posture while continuously working to strengthen it. With LevelBlue effectively managing your security risks, you can focus on your business.

Ranked as a leader by major analyst firms,[6] Check Point Email Security has the industry's highest catch rate for phishing and malware—including the most sophisticated evasive attacks.[7] Leveraging cutting-edge Natural Language Processing (NLP), it protects your cloud email against zero-day threats, compromised QR codes, malicious attachments, and more. This protection extends seamlessly across your entire collaboration suite, including SharePoint, Google Workspace, Slack, Teams, and many other apps. The solution is constantly evolving to become more adept. For instance, domain-based message authentication, reporting, and conformance (DMARC) capabilities are coming soon to protect email domain owners against spoofing.

Another benefit of the partnership between LevelBlue and Check Point is that you gain ready access to additional capabilities (such as security service edge) that you can leverage as your security program matures.

Contact your LevelBlue representative to learn more, or visit us at **levelblue.com**.

[6]Analyst reports where Check Point is top-ranked include: Forrester, The Forrester Wave™, Enterprise Email Security, Q2 2023; Omdia Universe Email Security Report 2024; Frost & Sullivan, Company of the Year Award, 2023; 2024 Miercom Security Benchmark.
[7]Miercom, 2024 Next Generation Firewall Benchmark Report.