

invisible
bits

INTACT Mail

EMAIL Isolation.
Next-gen EMAIL security.

It does not matter if your firewall is practically impenetrable.

It does not matter if you have a great antispam filter or the most efficient antivirus on the market.

It does not matter that the entire company has received complete training in cybersecurity.

It doesn't matter whatever you do.

One day, an infected e-mail will skip all the protections. And that day, despite all the warnings, there will be someone in your company willing to open it, to click on everything that is clickable to download and execute all attachments. And that day, you will know what chaos is.

Fortunately, there is INTACT Mail. INTACT Mail guarantees that users will never be able to access malicious elements hidden in the email, even if he/she wants.

INTACT Mail adds an **isolation layer** to avoid that employees devices get in touch with malicious elements. Ensure full mitigation of risks of infection and targeted attack from emails.

We bring the contents. You keep isolated.

The component integrated with the email client prevents the interaction with malicious email elements, even if attachments or links are already in the mailbox: it is isolated in a secure container, transparent to the end user.

How to prevent the 'Human Factor' from being the weakest link in the cybersecurity chain?

In spite of the multiple layers of security that you have implemented in your organization, from time to time an infected email manages to circumvent all of your defenses and reach the mailbox of any members of your company. At that time, starts the countdown to **denotate the bomb** inside your infrastructure.

Prevent employees from
accessing malicious emails.
Even if they want to.

INTACT Mail deploys an isolation layer in employees mailboxes supported by a secure shield in the cloud. Artificial Intelligence and behaviour analysis is executed over corporate email usage tasks.

Access to the company's email content is always done through an isolation layer that prevents exposure of the device to the threat. It is not possible to infect the devices even with targeted malware or exploits specifically designed for the endpoint.

The isolation layer **prevents interaction** with malicious elements even though they are already in the mailbox and connections with the final servers to avoid exploit kits and exploitation of the endpoint software, the employee's email environment is isolated from external threats.

The devices of the employees, desktops and mobiles, never interact directly with the malicious infrastructures, remaining intact against email threats.

Main Benefits

Optimize your investment

How do you justify your spending on security if an attack crosses your defenses and you do not face it quickly? Complemented with your current protection systems, INTACT Mail helps you optimize your investment.

Guarantee the continuity of your business

Thanks to INTACT Mail, you can neutralize advanced attacks and ensure the continuity of your business when the victim is a critical employee.

Hiding the endpoint

The employee never directly accesses final resources, attackers never receive direct connections from your infrastructure, keeping it isolated from infections, exploit kits and exposing the software versions that you use. Prevent targeted attacks to your corporate software stack.

Avoid reputation damage

In many occasions, corporate infections also spread rapidly to the outside, affecting your customers, suppliers and other contacts, and turning your company into the unwanted focus of the media.

Partner



Invisible Bits is a vendor specialized in innovative cybersecurity technologies to meet the specific needs of MSSPs and SOCs. Our technologies bring new approaches to solve nowadays cybersecurity requirements, providing intelligence to already deployed security infrastructures.

Key Features

Guaranteed tranquility

Even if the user tries to access or interact with any component of the malicious email, it will be impossible. INTACT Mail adds an isolation layer that prevents interaction with malicious contents, including links pointing to servers with malicious elements and exploit kits.

Isolation in a secure environment

INTACT Mail modifies the access to the external elements, so that they are always accessed through a secure shield. The shield analyzes and obtains the remote content, preventing the attackers from identifying the type of software that runs on the devices and delivering the contents only if they are safe, protecting the employee devices. Transparent and unattended.

Total protection

Ransomware, malicious documents and links, identity theft, targeted attacks and exploit kits: all work against the mail client or browsers. These threats will never come into contact with the employee's device; even if they are already in their mailbox. Thus avoiding exposure to the threat even though this is already inside the company. Employees will not be able to access malicious content **even if they want to**.

Real Artificial Intelligence

Our cloud analysis service uses soft techniques from Machine Learning and Threat Intelligence in different layers. We do not trust detection only by signatures and IOCs, and we rely on the intelligent analysis of malicious behaviors and patterns.

sales@invisiblebits.com
www.invisiblebits.com

World Trade Center Barcelona
East Building
08039 Barcelona
Spain

**invisible
bits**