EVERFOX

Securing Global Governments & Industries

Brochure

Rethink Cybersecurity

OUR MISSION

We protect our global customers against the most complex cyber challenges through innovative, high-assurance solutions that empower them to operate in an ever-changing cyber landscape.

Table of Contents

Proven Leader in Defense-grade Cybersecurity

Everfox brings more than 25 years of expertise supporting the unique and complex missions and objectives undertaken by the people who protect national security and mission-critical information globally. Intelligence communities, defense departments and civilian agencies require rapid and accurate ways to support their data-driven missions, and Everfox makes sure they are secure.

Our solutions bring together data security technologies – Cross Domain network protection, remote access and advanced monitoring combined with zero trust solutions – empowering our customers to use data where and how their people need it, safely.

The Everfox portfolio of cybersecurity solutions is designed to meet the most stringent security requirements, so you can achieve all of your mission objectives.

Resilient Security

Ensuring that your critical and sensitive data remains protected and guarded while enabling rapid authorized access and transfer.

Access Anywhere

Securely access mission-critical data whenever and wherever it's needed: air, space, land or sea, on network or in the cloud.

Advanced Analytics

Rapidly transforming information into accurate insights to inform the right actions from across the organization.

Unwavering Dedication

Resilience in the face of uncertainty is what sets Everfox apart.

We are dynamic, vigilant, and proactive in everything that we do. With the ability to not only adapt to any situation, but to come out on top.

Cross Domain Solutions

Cross Domain Solutions, whether they need to meet US regulations including Raise the Bar, UK NCSC design patterns with hardsec, or the equivalent stringent standards across the world, must do more than just protect networks. Of course, they must be engineered to **defeat the most sophisticated attacks,** even before they are known, but this must come with assurances that the protection will work, even when the defenses are themselves attacked.

The Everfox Cross Domain Solutions portfolio covers information exchange and remote access requirements, general purpose guards, hardsec bridges, and data diodes providing protocol breaks to protect the network level. Then, pipelined filters and Content Disarm and Reconstruction give data breaks that make content safe to handle. With high assurance appliances and cloud native services as platforms, all deployment options are available, ready to **deliver the security you need, no matter the application.**

Integrated Solutions to Support your Mission

Information superiority is key to the success of your mission.

Being better informed than your adversary and making sure the right people have access to the right information at the right time, ensure success. Achieving that requires connectivity, but losing control gives your adversary the advantage. They can learn your moves, disrupt your plans, and deny you the access you need. That's why Cross Domain Solutions are so important.

Additionally, we deliver monitoring and analytic solutions that ensure systems run smoothly, protecting against mistakes and willful damage from within.

Advanced security solutions for global industries.

Continuous, safe operation is the essential requirement for any production system. However, the overriding concern for safety rules out invasive security solutions, such as aggressive monitoring and continuous patching. Everfox's security solutions provide an answer, as they are deployed at the edge, enabling information sharing and remote access while providing a solid defense against attack.

Keeping sensitive personal information safe

Personal information about your clients and customers is a tempting target for cyber criminals, whether it's for fraud or ransomware. Know Your Customer and other regulatory requirements increase the need to hold this information. It also means that any failure to protect it brings harsh penalties on top of potential reputational damage.

Your systems must be able to handle this information and you must be sure that the security built into and around those systems is able to protect it.

That's where Everfox's security solutions differ from more conventional approaches. They don't just offer a solid defense but are implemented in a way that gives you complete confidence in your defenses.

Information eXchange (iX)

Benefits:

Simple Setup

Intuitive GUI and configuration – up and running in under 30 minutes

Multi-Channelled

Supports multiple data channels, able to use different protocols and handle different data formats

Protocol Break

Enforces a protocol break to block network level attacks

Data Break

Provides a data break so potentially hostile data never reaches its target, even in complex formats like Office & PDF

Blocks Covert Data

Stops covert infiltration of malware and leakage of sensitive data, including steganography, and smashes covert Command and Control

The iX Appliance supports information exchange, while keeping networks separate through a protocol break and making sure delivered data is safe to handle with a data break.

Deployed inline on a network perimeter, Everfox's Information eXchange (iX) Appliance enables the secure transfer of email, web API traffic, file transfers and activity logs.

The appliance can be configured to act as a protocol proxy, which is split into two to provide the protocol break, for SMTP email or to support data transfers using HTTP, and for basic TCP/UDP protocols. The data break implements Everfox Content Disarm and Reconstruction for both structured and unstructured data.

As an off-the-shelf appliance, the iX only needs to be configured with protocol parameters, data format selection and any application specific schemas for structured data. The appliance is deployed on a pair of servers, with the proxy and CDR functionality distributed across them. This reduces the attack surface and so maximizes the strength of network separation.

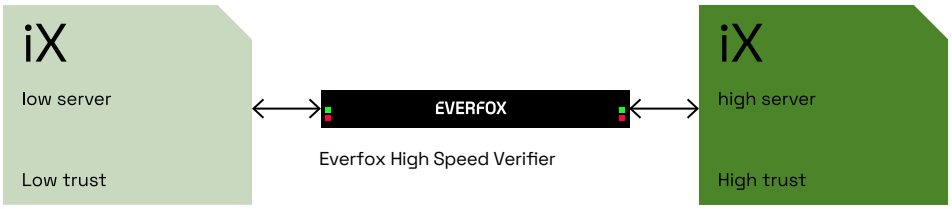
Comprehensive malware protection

Located at the network perimeter, the iX operates inline to eliminate potential threats from business content, including unstructured formats like Office and PDF, and application-specific structured data like XML and JSON.

Hardware logic verification

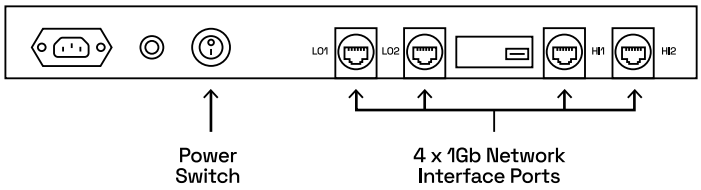
For systems that face the most sophisticated threats and require hardsec protection, the two iX severs can be deployed connected via Everfox's High Speed Verifier (HSV).

The HSV provides independent verification implemented in hardware logic of the data being transferred. This means there's no software to make it vulnerable to attack and its simplicity means its effectiveness can be independently confirmed.



Front View

Rear View



High Speed Verifier (HSV)

The Everfox High Speed Verifier (HSV) is a hardsec device that connects two networks together. It implements a protocol break and data break entirely in hardware logic. This means no software vulnerabilities can undermine the control it imposes.

The HSV can also be deployed between two servers of an Information eXchange (iX) Appliances, boosting the assurance of general purpose Cross Domain applications to hardsec levels.

Hardware logic data break

The logic verifier inside the HSV deals with a simple protocol and a simple data format for structured data. Application protocols and data formats are converted by software, but the logic verifies that the simple protocol is followed, and the data meets the strong constraints defined by the application.

The data received is never delivered, giving an assured data break. This data break is built on top of the protocol break that comes from converting the application protocol into the simple protocol that's implemented by the logic, assuring it cannot be bypassed.

Key benefits:

Robust Security

It relies on simple logic, not software

Simple Solution

Making it easy to gain confidence in its effectiveness

Protocol Break

Hardware logic enforces a protocol break to block network level attacks

Data Break

Hardware logic verifies data is correctly structured

Application Specific Control

Enforces data semantic constraints that can be configured to the precise needs of the application

Data Guard

Key benefits:

Full Protocol Break

Using common criteria-evaluated platform

Highly Customizable

Data validation rules are highly customizable for maximum flexibility

High Availability

Supports non-stop operation

Reduces Costs

Provides the strength of an air gap with the convenience of a network connection

High Assurance Inspection & Sanitization

Byte-level content inspection and sanitization

Providing defense-grade control over data transfers

The Everfox Data Guard is a highly customizable platform for moving data between networks that are otherwise kept separate. It can be used to build Cross Domain Solutions and other high assurance defenses for critical networks, meeting information sharing and remote access requirements.

Build your solution by selecting from a range of protocol handlers and data filters. These are combined to fit the precise needs of each application. Data can be manipulated and filtered in a variety of ways, including being made safe through the use of Content Disarm and Reconstruction.

A trusted operating system ensures data always takes the correct path through the selected components. This allows custom components to be added without undermining the overall security of the guard.

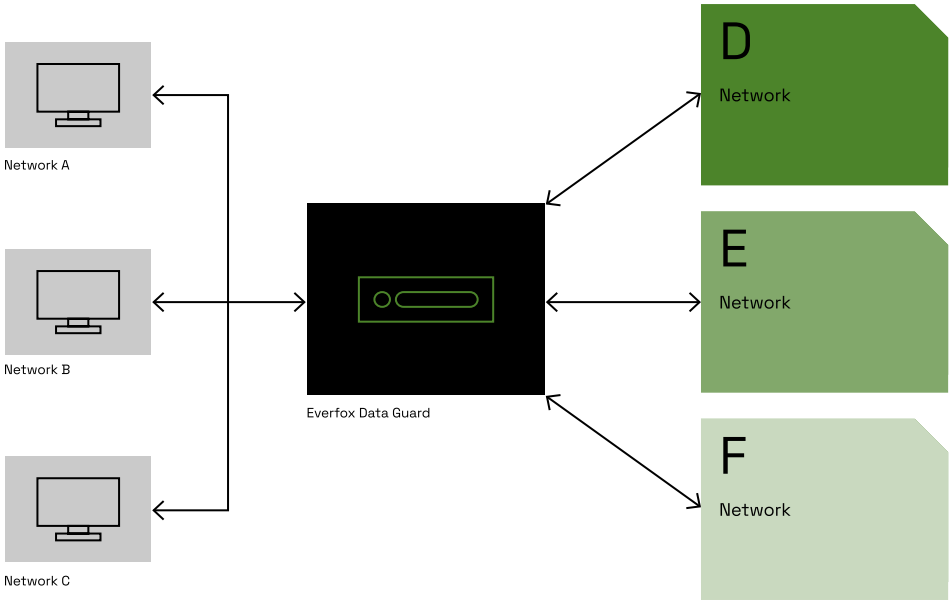
A flexible approach

The Data Guard is highly flexible in its secure approach to high-assurance data movement through the robust security policies within adaptors, plugins and the filtering process. The rule engine provides APIs to handle multiple rich data types.

Secure data transfer

The Everfox Data Guard enables secure data and file transfers between otherwise disconnected networks. Supporting structured (e.g. JSON and XML/SOAP,) unstructured data (imagery, Office, and PDF etc) and streaming data formats such as video. Different constraints can be applied depending on the direction of travel. The Data Guard can connect multiple networks, and flows can be made strictly one-way.

The Data Guard is built on a trusted operating system – Red Hat Enterprise Linux with enhanced SELinux modules —which enforces network separation and ensures data constraints are always applied, allowing it to be used in highly regulated environments.



Data Diode

The Everfox Data Diode enables rapid data transfers from one network to another, while ensuring that no information passes in the opposite direction.

The Data Diode can be used to get information out of a critical network without introducing any means by which that network can be attacked. Additionally, it can be used to get data into a network that handles highly sensitive information without risking a leak.

With the Data Diode, you can be confident that there are no reverse information flows. This is due to the physical properties of fiber optic networking electronics, rather than any software.

That means you can get the monitoring data, open source intelligence, software updates, etc. that are so essential to your operation without endangering the critical system.

Key benefits:

Secure One Way Transfer

Rapid, secure one-way and automated transfer of highly complex data with optical isolation

Automated Transfer

No need for a manual air gap

High Assurance Security

Physical properties ensure no reverse information flows

Lower Total Cost of Ownership

Replaces air gaps, reducing operational costs and giving improved security

Simple Setup

Rapid and low risk integration into network infrastructure

Policy Engine Guard

The Everfox Policy Engine Guard is used by organizations that need to tightly control business content passing across an external boundary or between separate internal zones over email, web or file transfer. It defends against known malware and accidental data loss by focusing on business content.

Deep content inspection

The Policy Engine Guard intercepts content at the boundary point and uses Deep Content Inspection (DCI) to examine it for the presence of known threats and the possibility of accidental data loss. Embedded content, including archives, is unwrapped to gain a complete picture of the data being carried.

Key benefits:

Stop Malware and Data Loss

Protects organizations from accidental data loss and known malware

Validation

Of S/MIME signed messages (email) and address validation (email) and NTLM authentication of users (web)

Policy Based Identification

Ability to apply policy based on identification of unstructured or structured protective marketing / security labels and user clearances

Modernizing Security with a Zero Trust Approach

Within complex security ecosystems, Zero Trust cannot be merely a compliance exercise. Adding more point products and policies only makes security unmanageable. You need a more unified security platform.

Everfox solutions go beyond static access controls to truly transform your security. We offer a complete security platform that spans the pillars of Zero Trust to provide both inbound threat protection and outbound data loss prevention.

Everfox solutions support governments and industries globally, at home, at secured facilities and at the tactical edge.

Content Disarm & Reconstruction (CDR)

Stop known and unknown threats, zero-day attacks and malware. Rather than trying to detect malware, Everfox CDR technology believes that nothing can be trusted.

That's why our CDR is a game-changer for mitigating against the threat of even the most advanced zero-day attacks and exploits.

Pivoting from detection to prevention is especially important with the evolution in hybrid work forces and their resultant usage of content and electronic information everywhere.

Key benefits:

Defends Against Advanced Threats

Stops ransomware and zero-day threats without the need for the latest patches

Reduce Costs

Frees up SOC teams from day one, with zero false positives

Enhanced User Experience

Reduces latency by not subjecting incoming files to multiple scanners, sandboxing or flattening

Choice of Deployment

On-premise, cloud or application

Defends a Wide Range of Attack Vectors:

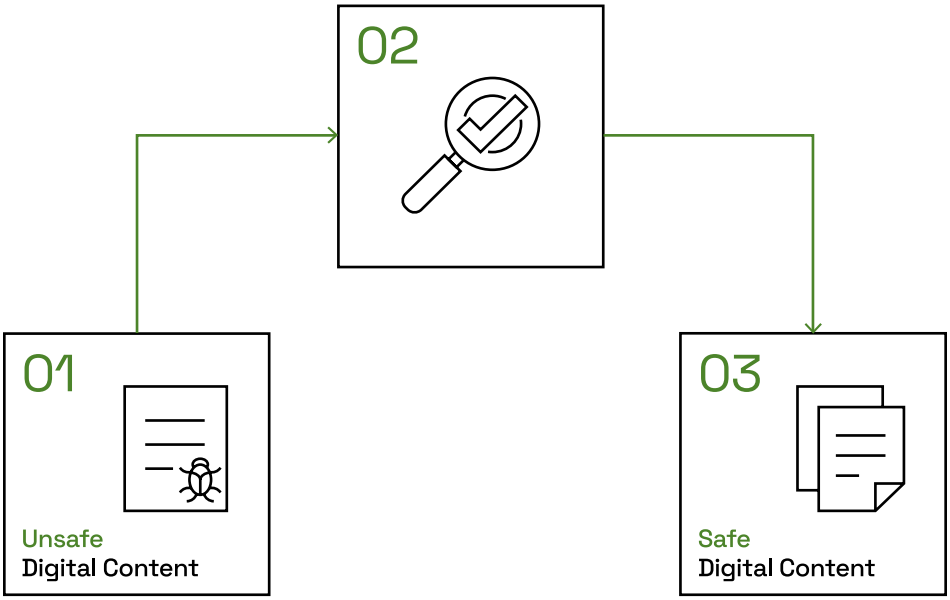
Email	Web Browsing
Chat	File Sharing
File Uploading	Applications

How Everfox CDR works

01. Extracting the valid business information from files (either discarding or storing the originals).

02. Verifying the extracted information is well-structured.

03. Building new, fully functional files to carry the information to its destination.



CDR for Mail: Microsoft 365

Nine out of ten data security breaches start with an email, resulting in organizational disruption, financial damage, or data loss. Which is why a new level of protection is required to match the threats of today's ever evolving cyber landscape.

Get comprehensive protection for your most critical business investment – Microsoft Office 365.

Protecting Microsoft 365 emails, users and data

Email is one of the most popular attack vectors – and one of the most difficult to secure. CDR for Mail: Microsoft 365 enhances email security with simple, fast & seamless protection for users' inboxes.

It's time to transform your email security

When using Microsoft Office 365, CDR for Mail cleans all email messages and attachments when mail is being processed by Microsoft 365. The original data carrying the information is discarded along with any threat. Completely brand-new messages and attachments are then created and delivered to the user.

Nothing gets delivered but safe content. Attackers cannot get in and the business gets only what it needs.

Key benefits:

World Class Level of Email Protection

Defeats advanced malware with prevention CDR technology

Protects All Inboxes

Incoming, outgoing, and internal

Set-up In Minutes

Getting started is quick and easy

Seamless Integration

Works with existing technology and boundary defenses

Reliable

Native technology with an average uptime of 99.99%

Data Protection

From theft and steganography

Application eXchange APIs (AX)

Everfox Application eXchange (AX) is a set of API's that developers can leverage to access CDR-as-a-Service (CDRaaS) to integrate unmatched threat protection into their workflows and applications.

Built on serverless computing and microservices for limitless scalability, CDRaaS ensures that all digital content is threat-free.

Key benefits:

Secure One Way Transfer

Rapid, secure one-way and automated transfer of highly complex data with optical isolation

Automated Transfer

No need for a manual air gap

High Assurance Security

Physical properties ensure no reverse information flows

Lower Total Cost of Ownership

Replaces air gaps, reducing operational costs and giving improved security

Simple Setup

Rapid and low risk integration into network infrastructure

Digitally pure content

The CDR content transformation engine will transform OfficeX, PDF, image files and more, rendering them free from evasive, zero-day, known and unknown threats.

THE APPLICATION EXCHANGE API IS AVAILABLE IN 3 VARIANTS:

The Instant API

Enables simple uploading and immediate downloading, doesn't require any additional infrastructure and is suitable for content that is under 5MB.

The Async API

Supports file sizes up to 250MB and more complex content. It enables large files to be processed and allows more advanced scenarios such as uploading from one system and then downloading the safe content from a separate system.

The S3 API

Lets us pull and push content from and to your S3 buckets. Just tell us how to access them, and we'll do the rest.

Gateway eXtension (GX)

Existing perimeter web defenses (web gateways & firewalls) are failing to cope with the onslaught of known, unknown, and zero-day threats concealed in business documents and images.

Extend the capability of your perimeter web defense using the Everfox Gateway eXtension (GX) to combat these threats.

Integrate seamlessly with existing defenses

In addition to being able to integrate seamlessly with existing perimeter web defenses, secure web gateways, next-generation firewalls, and web application firewalls, the GX can also link to ICAP protocol-enabled next-generation firewalls. Providing total protection from content-borne threats crossing the web boundary at a low cost and risk.

No more zero-day content threats

- Has "swivel chair" access to two or more disconnected networks
- Uses a form of remote desktop access, including Garrison SAVI, from their protected network to reach a virtual desktop infrastructure on an untrusted connected network
- Accesses the internet from a protected system using a Garrison SAVI remote browsing solution.

Existing perimeter web defenses (web gateways & firewalls) are failing to cope with the onslaught of known, unknown, and zero-day threats concealed in business documents and images.

Key benefits:

Secure One Way Transfer

Rapid, secure one-way and automated transfer of highly complex data with optical isolation

Automated Transfer

No need for a manual air gap

High Assurance Security

Physical properties ensure no reverse information flows

Lower Total Cost of Ownership

Replaces air gaps, reducing operational costs and giving improved security

Simple Setup

Rapid and low risk integration into network infrastructure

File eXchange (PX)

Everfox File eXchange (PX) is an exchange application, allowing a user with a footprint on two separate networks to send files from one network to themselves on the other network.

It is deployed with an Information eXchange (iX) appliance to ensure delivered files are rendered safe by our Content Disarm and Reconstruction (CDR) , and/or a Policy Engine Guard for Deep Content Inspection and rigorous policy enforcement.

The PX can be employed where the user:

The Policy Engine Guard intercepts content at the boundary point and uses Deep Content Inspection (DCI) to examine it for the presence of known threats and the possibility of accidental data loss. Embedded content, including archives, is unwrapped to gain a complete picture of the data being carried.

The Policy Engine Guard is ideally suited to systems in government, law enforcement, defense and regulated industries.

Key benefits:

Secure and Reliant

Secure file transfers between isolated networks malware

Simple Set-up

Software package installs with minimal configuration

Easy to Use

Web app or close integration with Garrison remote browsing

Choice of platforms

Windows or Linux

Unveiling Insider Risk Cybersecurity

Insider Risk is a critical component of a holistic cybersecurity strategy, addressing vulnerabilities that may not be ad visible as external threats. The biggest risk to your data comes from within.

Everfox Insider Protection solutions allow you to uncover internal threats before the loss becomes real. We combine visibility and analytics to help you understand how users interact with critical data and stop risky behaviors “left of loss.”

By implementing Insider Risk security measures, **you can better protect your sensitive data, maintain compliance and fortify your defenses against a range of insider risks.**

Insider Risk

Collect, Explore and Gain Insight.

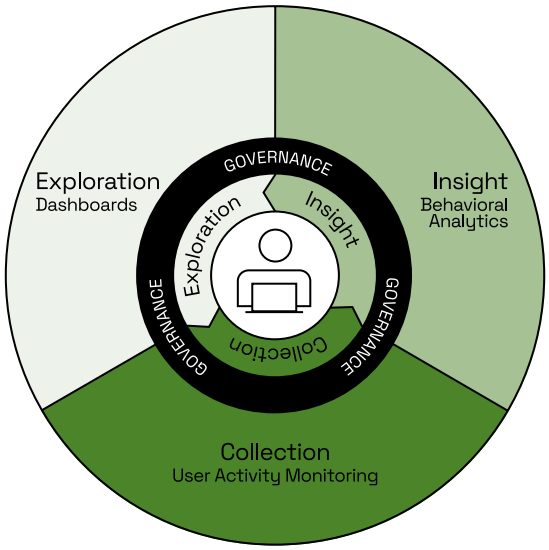
Collect behavioral data from channels such as web, file operations, keyboards and email.

Explore meaningful data using a powerful dashboard built for analysts, by analysts.

Gain Insight with powerful analytics to understand and rapidly respond to risky behaviors before harmful events occur.

Govern to ensure the integrity and effectiveness of the insider risk inquiry and response processes.

Optimize operations with centralized analyst audit, maintain privacy, comply with best practices such as Role Based Access.



Key benefits:

High Level Monitoring

Monitor a broad set of data sources and activities

Customization

Custom configuration to suit specific requirements

Analytics

In-depth analytics to ensure rapid response to risky behaviors

Top Data Collection

Collect behavioral data from multiple channels

Internal and External

Protect your workforce from internal and external threats

Data Protection

Safeguards your data and critical assets

Increased Visibility

Increases visibility and user monitoring

With Everfox Insider Risk you can:

Establish undeniable attribution

Video collection and playback helps expedite investigation, allowing for attribution as intent and is admissible in a court of law.

Safeguard your investment

Prevent overreach with the ability to control, watch, and audit investigators. Eliminate biases with anonymized data for investigation integrity.

Optimize your workflows

Always-on, highly customizable monitoring and enforcement allows prioritization of the riskiest users to prevent breaches before they occur.

Protect your workforce

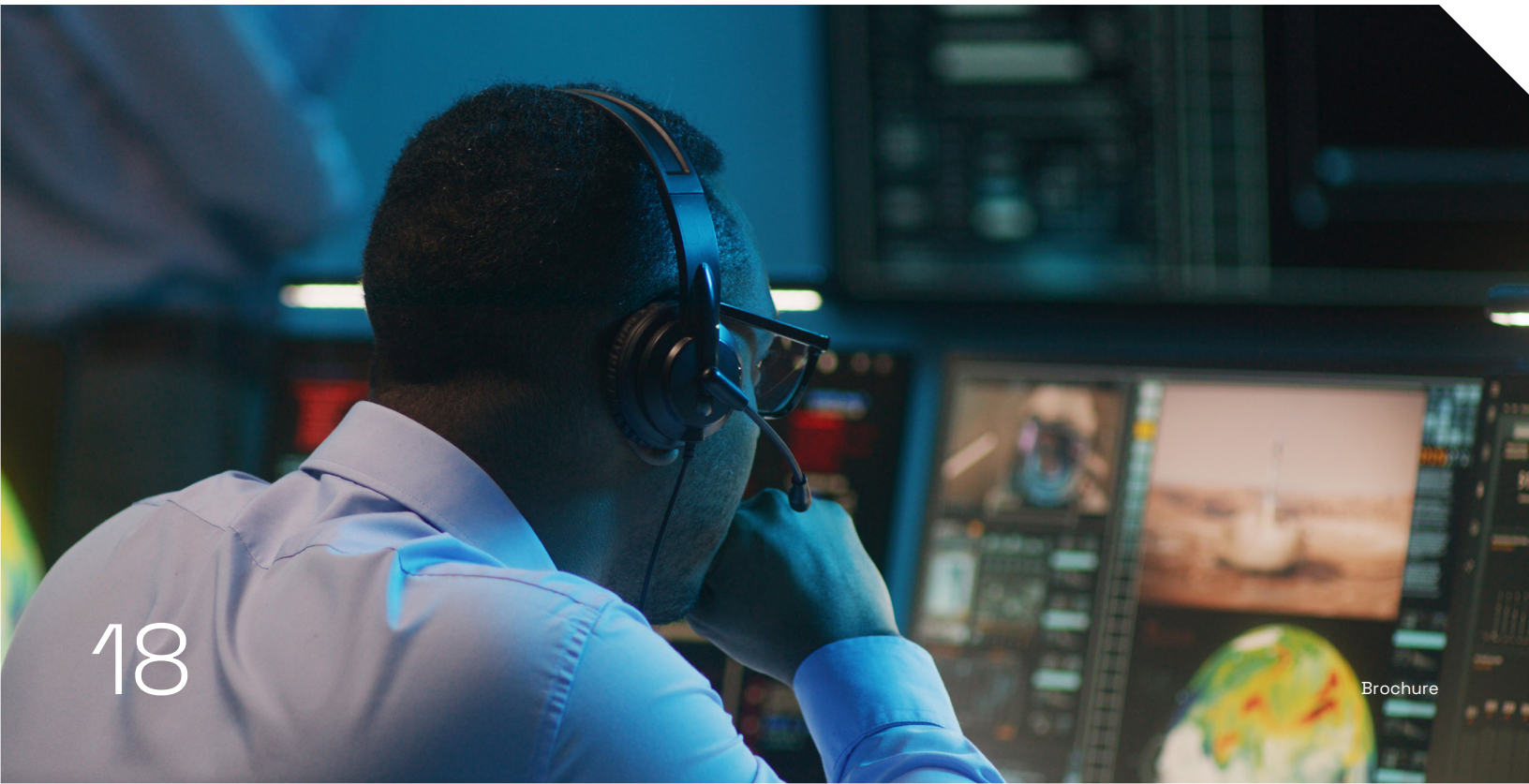
Leverage detailed forensics to quickly understand intent and exonerate employees of wrongdoing.

Identify your riskiest users

Monitor a broad set of data sources and activities to uncover patterns of insider risk rather than individual events.

Customize your program

Prioritize and monitor what matters most to your organization through custom configuration.



Intelligent. Resilient. Dynamic.

Everfox

We exist to protect what matters. We stop cyber attackers taking control of our customers' networks and prevent leaks of sensitive information.

Our software, services and hardware solutions enable our customers to focus on their mission. Our customers are depended upon across the globe and as a result are at the scrutiny of the most advanced form of cyber-attacks. We help to keep them operational at all times.

We are proud to provide leading Cross Domain, threat protection and Insider Risk solutions globally, as we continue to lead the way through relentless innovation and commitment to our customers.

From national defense to regulated industries, safeguarding the world's most valuable networks and digital assets has never been more crucial. To achieve this requires a level of expertise that we believe is unmatched. A level of expertise that we have.

We innovate. We invest. We achieve.

25+
Years of empowering governments and enterprise organizations to use data safely, where and however their people need it.

100
Countries supported globally by Everfox solutions.

150+
Granted and pending patents.

Beyond secure – we define the future of cyber resilience

EVERFOX

About Everfox

Everfox, formerly Forcepoint Federal, has been a trailblazer in defense-grade cybersecurity for more than two decades. Leading the way in delivering innovative, high-assurance solutions. But we're just getting started.

Learn More: www.everfox.com