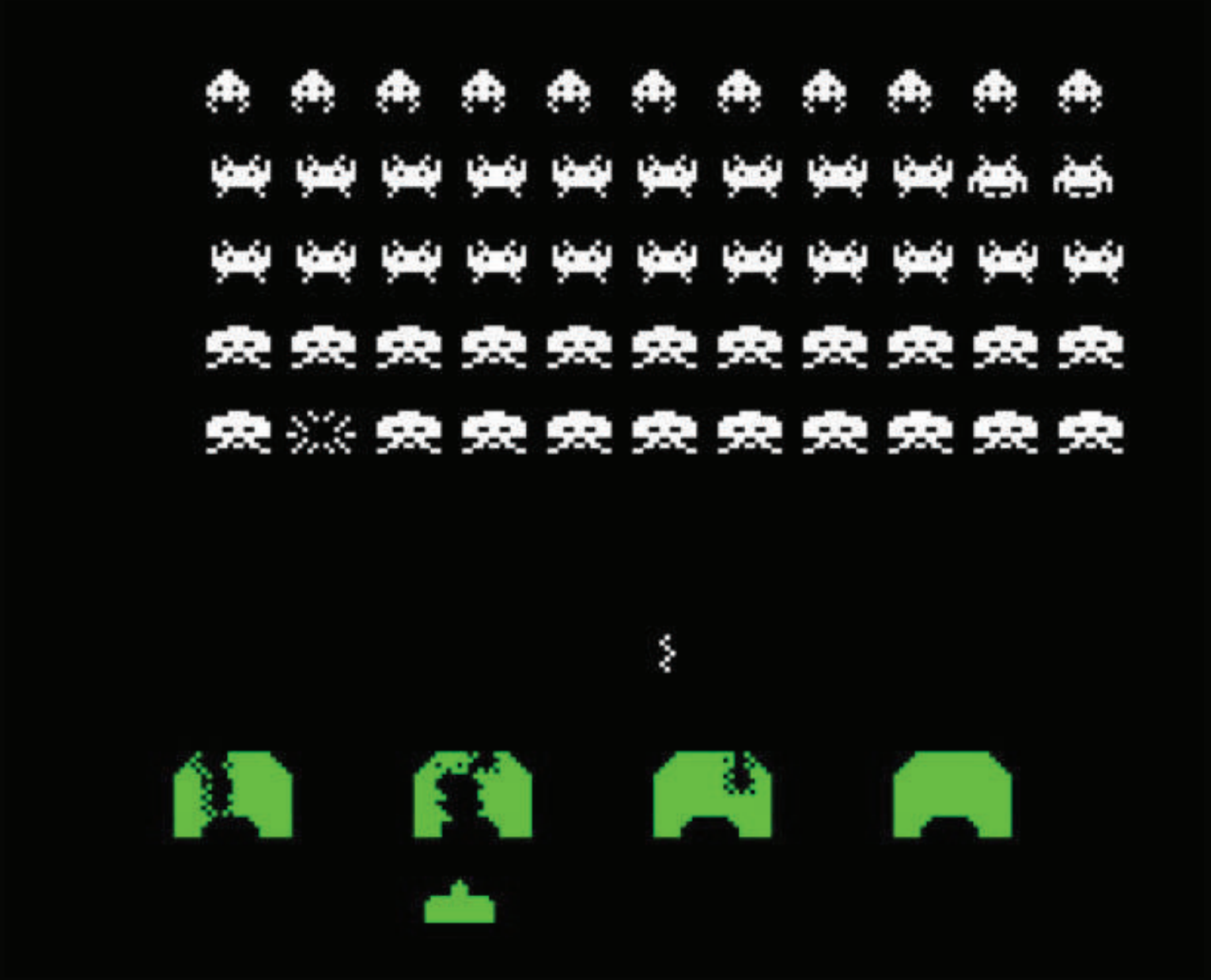
REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

IT'S YOUR UNIVERSE.

What's your plan once they're through your defense?



THE FINAL LINE OF DEFENSE.

We protect against the threats that get past AV, MDM, EDR & VPN.

NON-INVASIVE.

We don't need to monitor sites visited or user activity to protect your data.

SCALEABLE.

Quick, lightweight and easy to install and manage, across the enterprise.

Trusted by over 5 million users. We do not detect, We scramble. SentryBay compliments your existing Antivirus, MDM, EDR and VPN solutions. Regardless of existing threats, we safeguard data and ensure you meet legal compliance standards.

REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

Most CISOs, MSSPs and Senior IT Architects make use of AV, EDR, MDM and/or VPNs.
Here are some of the vulnerabilities that we help you prevent.

	Typical Antivirus	Typical Endpoint Detection & Response	Typical Mobile Device Management	Typical VPN	SentryBay Armored Client
Malware Detection & Machine Learning	✓	✓	–	–	N/A*
Device Management	–	–	✓	–	–
Anti Keylogging	–	–	–	–	✓
Anti Screen Capture	–	–	–	–	✓
Locked Down Browser	–	–	–	–	✓
MITM / MITB Protection	–	–	–	–	✓
Protection Against RDP Double Hop	–	–	–	–	✓
DLL / Code Hooking Injection	–	–	–	–	✓
Protection Against DNS Attack	–	–	–	–	✓
Secures BYOD Devices	–	–	–	–	✓
Secures Data on Legacy Applications	–	–	–	–	✓
Secures VDI & Secures VPN Connections	–	–	–	–	✓
Secures Corporate Applications	–	–	–	–	✓
Secures Saas & Web Apps	–	–	–	–	✓

The #1 hacking tool globally is still key-logging and the use of screen capture malware.
This is where SentryBay compliments your existing threat management and data security architecture.
We prevent threats from exfiltrating data from protected applications. We are the last line of defense.

While AV and EDR are about detection and response we differ in that we scramble and conceal input and output data. When a keylogger or screen scraper gets through your standard defences, we are the final level of security. Our patent-protected anti-keylogging and anti-screen capture technology makes us the perfect complimentary partner to AV and EDR.

*Our solution does not rely on detection from a known database or the use of heuristics.

REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

Key Features

Secure Remote Work

The SentryBay Armored Client prevents malware from accessing sensitive data across managed, unmanaged and BYOD. We secure remote access solutions (like Citrix and VMware), corporate applications (like Microsoft 365) and Saas and Web Apps (like Salesforce).

Guarantee User Privacy

Staff and users don't like the idea that you're watching their every move online. The SentryBay Armored Client doesn't need to monitor what websites your users visit or their activity. It blocks keyloggers, screen scrapers, prevents DLL code injection and provides a clean enforcement mechanism to ensure confidence in the security.

Delivery To The Board

In businesses where you have a large number of BYOD you have to ensure that data cannot be exfiltrated from the system. The cost of a full EDR + managed devices, plus hardware, license fees and deployment, P&P + provision for unreturned devices, other CAPEX costs and high staff turnover rates, are going to raise some eyebrows at the next board meeting. A major reason for our success has been affordability and ROI.

Compliance

Regardless of existing threats, we safeguard data and ensure you meet legal compliance standards across BYOD, managed and unmanaged devices. Regulations such as GDPR, PCI, PSD2, HIPAA and more.

Lightweight but highly secure, SentryBay is configured to protect applications important to the enterprise. Multiple protections to the application and operating system are underpinned by patented kernel level keylogging protection.

Secure Data & Apps

Secure Legacy Systems

Secure Remote Work

Keep The Board Happy

REDITE.
Cyber & Data Security

AUTHORISED DISTRIBUTOR SentryBay ASIA PACIFIC

Key Products

Armored Client

Adds multiple security layers to key applications on corporate/BYOD devices, securely wrapping:

Remote Access solutions
(Citrix, VMWare etc)
Corporate application suite
SaaS applications

Threats Combated:
Prevents keylogging (incl. kernel), MITM/MITB, screen capture, dll injection, ensures process integrity, prevents RDP/double-hopping etc.

Features/Benefits:
- Advanced security to protect all logins, data transfer and transactions - regardless of the security state of the endpoint
- Prevents data breaches and fraud
- Branded to partner/customer, each tab can protect designated range of apps/services
- Meets range of compliance requirements, FFIEC layered security, HIPAA, PCI etc.

Armored Browser

Dedicated, locked down browser/endpoint software which securely wraps SaaS applications, infused with multiple, layered protections.

Online Banking / brokerage / wealth management, Healthcare platforms, Government/council/tax portals, Legal/accounting platforms

Threats Combated:
Man-in-the-middle (MITM/MITB), keylogging (incl. kernel), screen capture, MITB, phishing, sophisticated malware, DLL injection.

Features/Benefits:
- Advanced security to protect all logins, data transfer and transactions - regardless of the security state of the endpoint
- Prevents data breaches and fraud
- Branded to partner/customer, each tab can protect designated range of apps/services
- Meets range of compliance requirements, FFIEC layered security, HIPAA, PCI etc.

BankSafe

Endpoint software securing online banking login and transactions. Works with any browser.

- Personal online banking
- Business / corporate banking
- Online brokerage / trading / forex
- Insurance / wealth management portals

Banksafe prevents keylogging (incl. kernel), screen capture, MITB, phishing, sophisticated malware, ransomware.

Features/Benefits:
- Meets FFIEC layered security compliance
- Reduces online banking, Card-Not-Present and identity theft-based fraud
- Deeper protections - yet more user friendly - than Trusteer Rapport
- Works alongside any other endpoint security software, and with 2FA.

CryptoSentry

Stopping the encryption of files.
Endpoint anti-ransomware software providing proactive protection.
Prevents loss of data files (including emails, photos & documents) as well as business data (including financial, personnel, operational data.)

Features/Benefits:
- Protects against file encrypting ransomware not detected by anti-virus
- Identifies and proactively blocks any illegitimate attempt to encrypt files.
- Software provides alerts and relevant information to users.
- No user education or action required
- Software can be branded to partner, and level of customer notifications and interactions can be customised
- The app is downloaded & installed from the customer portal in seconds, providing a branded icon, without requiring configuration or customization.

Credential Monitoring:

- Optional real-time check on login credentials on the deep/dark web.

- Checks billions of credentials from aggregated data sets from SentryBay & many other suppliers/sources.

REQUEST A SENTRYBAY PRODUCT DEMO

CONTACT US
1300 010 733
redite.co
paul@redite.co

You can have all the defenses in the world,
but once an attacker has your credentials, it's

GAME OVER