Elevating Your Endpoint to the Next Level of Security

- **Andrew Smith**
- *CHANNEL ACCOUNT MANAGER*

- andrew.smith@eset.com

As soon as the internet was born, the world immediately became smaller.

bot zero trust zero-day clickjacking EDR APT

keylogging machine learning IP address

captcha vulnerability

patch management endpoint detection blockchain EDR

ransomware deny list

malware breach brute force attack

whitelist

account hijacking

advanced persistent threat deny list SIEM

data mining

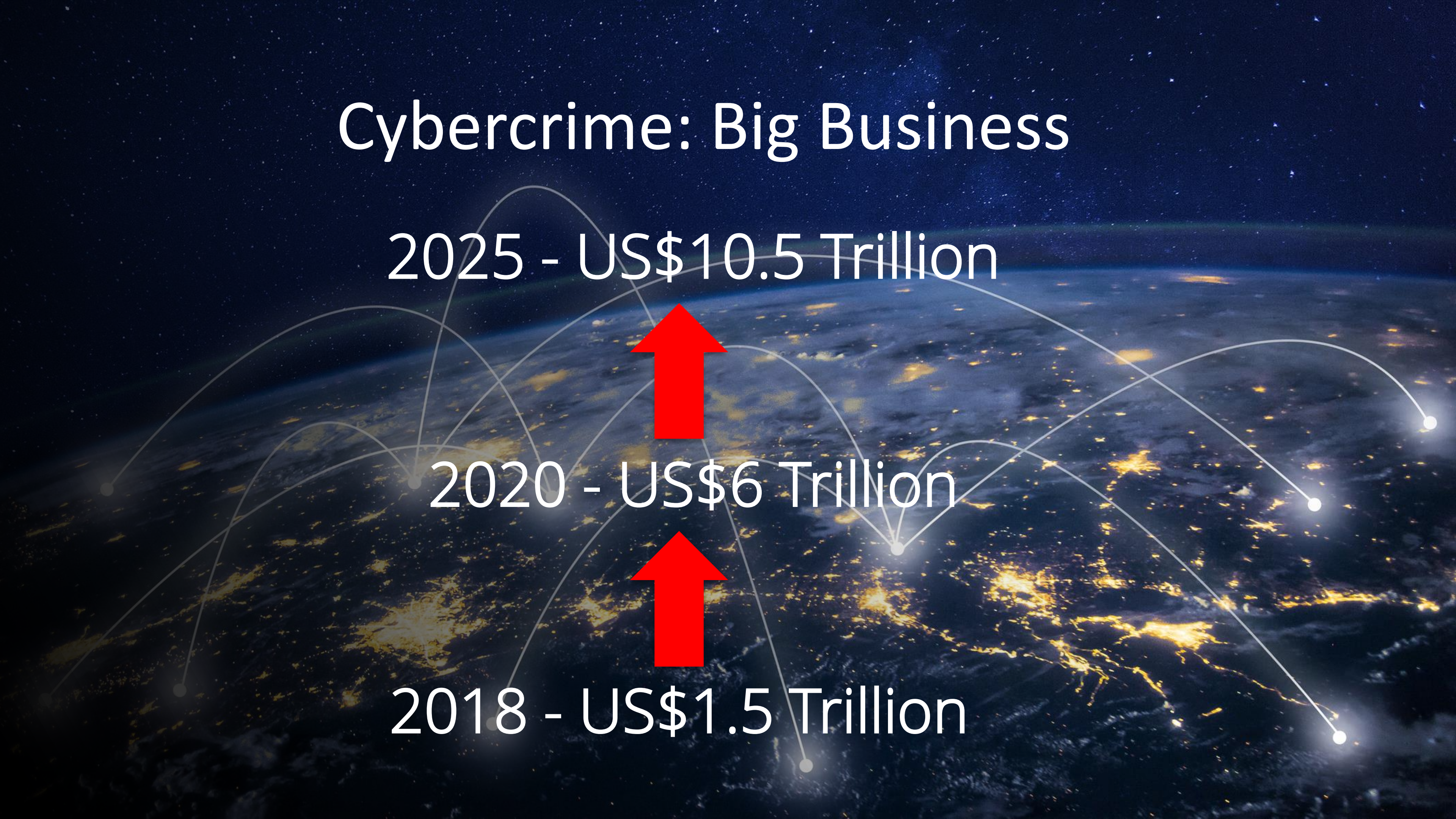
rootkit attack vector

virus domain XDR MITRE

digital forensics AI security sandboxing

encryption DDoS exploit DoS

Cybercrime: Big Business



2025 - US$10.5 Trillion

↑

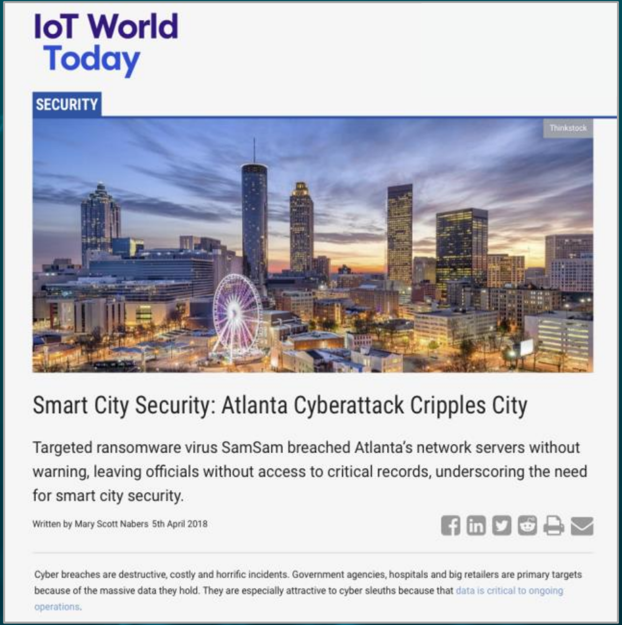
2020 - US$6 Trillion

↑

2018 - US$1.5 Trillion

“I launch cyberattacks because that’s where the money is.”

Was this the monetization tipping point?



IoT World Today

SECURITY

Thinkstock

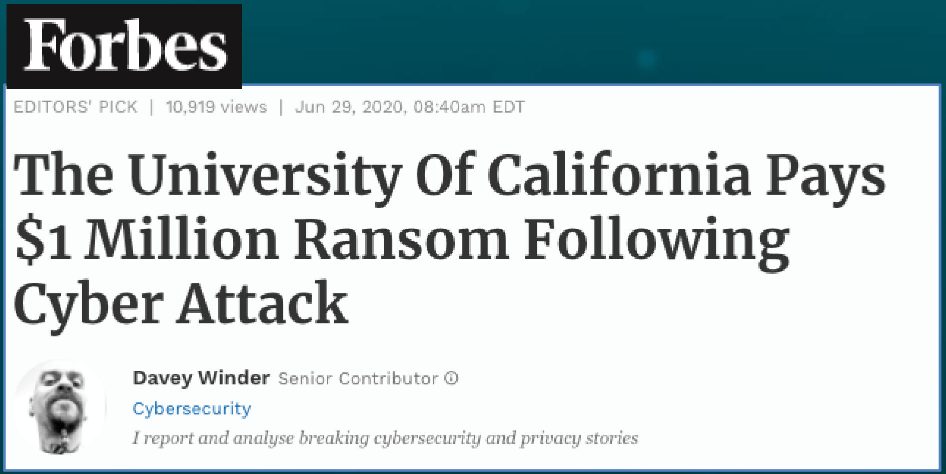
Smart City Security: Atlanta Cyberattack Cripples City

Targeted ransomware virus SamSam breached Atlanta's network servers without warning, leaving officials without access to critical records, underscoring the need for smart city security.

Written by Mary Scott Nabers 5th April 2018

Cyber breaches are destructive, costly and horrific incidents. Government agencies, hospitals and big retailers are primary targets because of the massive data they hold. They are especially attractive to cyber sleuths because that data is critical to ongoing operations.

Ransomware demands – 2020



Forbes

EDITORS' PICK | 10,919 views | Jun 29, 2020, 08:40am EDT

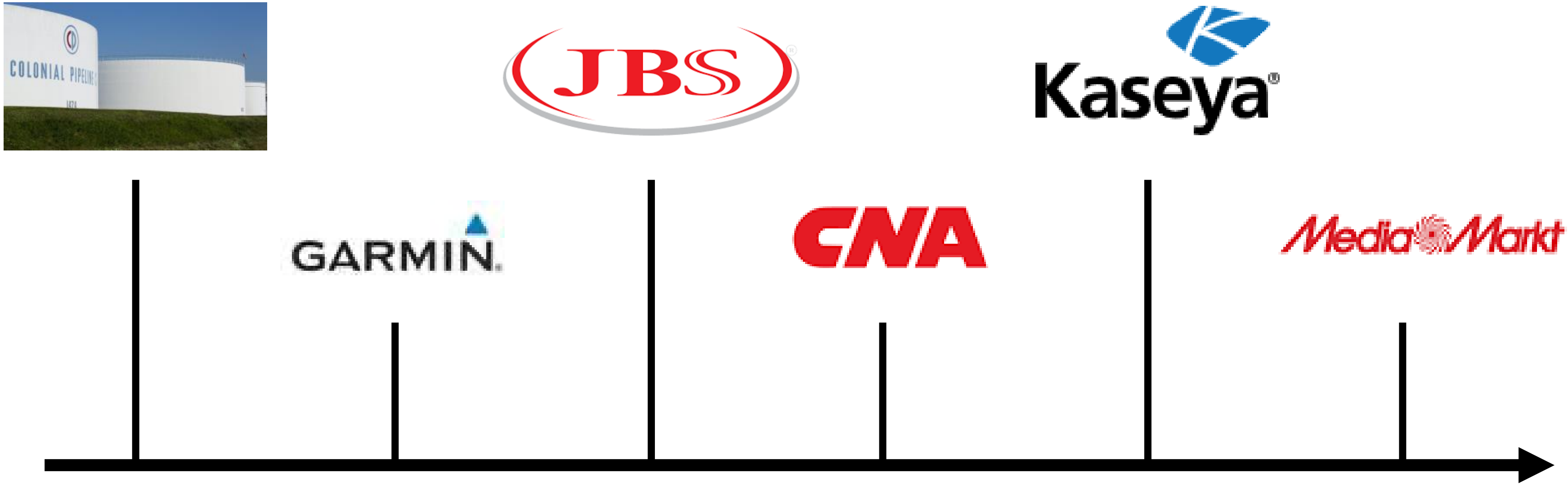
The University Of California Pays $1 Million Ransom Following Cyber Attack

Davey Winder Senior Contributor ⓘ

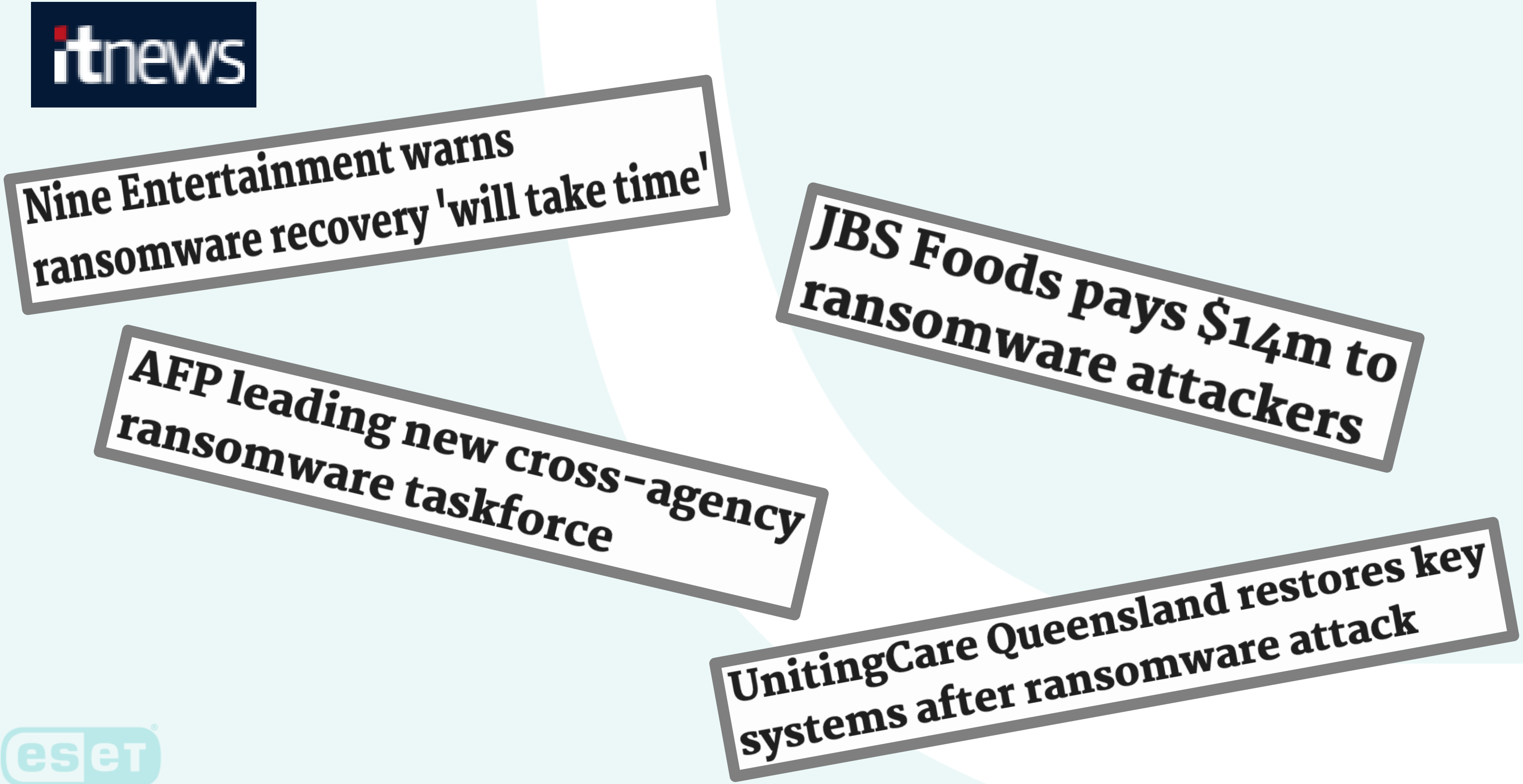
Cybersecurity

I report and analyse breaking cybersecurity and privacy stories

The escalating demands - 2021



$4.4m $10m $14m $40m $70m $240m



itnews

Nine Entertainment warns ransomware recovery 'will take time'

JBS Foods pays $14m to ransomware attackers

AFP leading new cross-agency ransomware taskforce

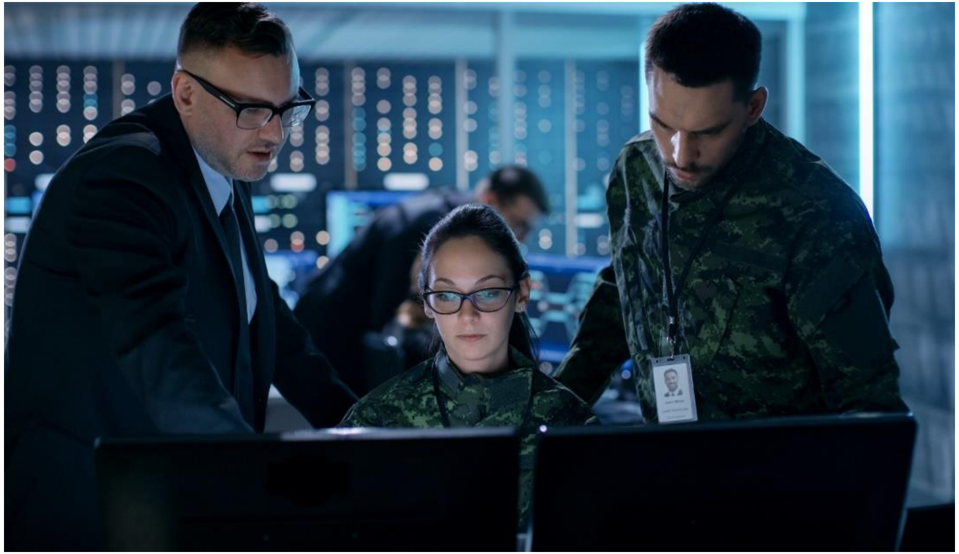
UnitingCare Queensland restores key systems after ransomware attack

The change in attack process

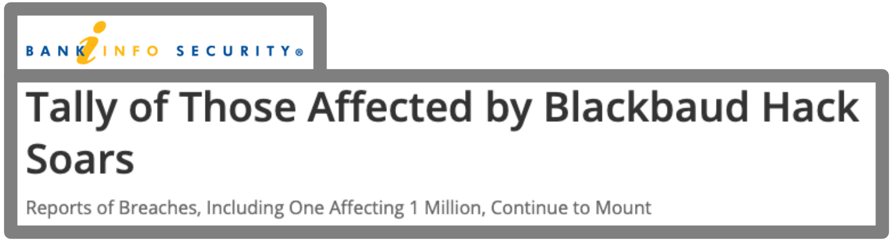
- Identify targets
- Initial compromise
- Establish foothold
- Privileges and lateral movement
- Data exfiltration
- Disable security systems
- Execution of malware

"I launch cyberattacks because that's my job."

"I launch cyberattacks because that's what my government tells me to do."

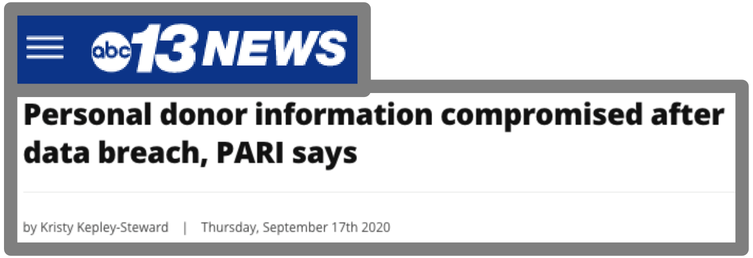


blackbaud™



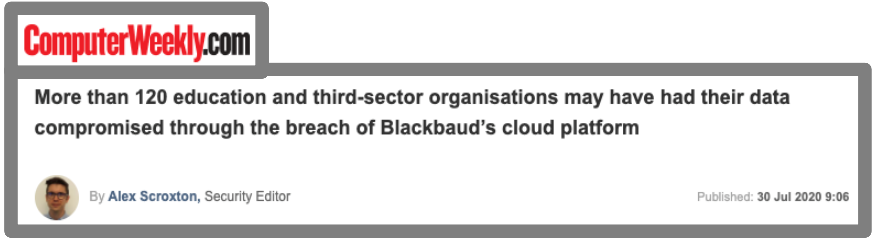
Tally of Those Affected by Blackbaud Hack Soars

Reports of Breaches, Including One Affecting 1 Million, Continue to Mount



Personal donor information compromised after data breach, PARI says

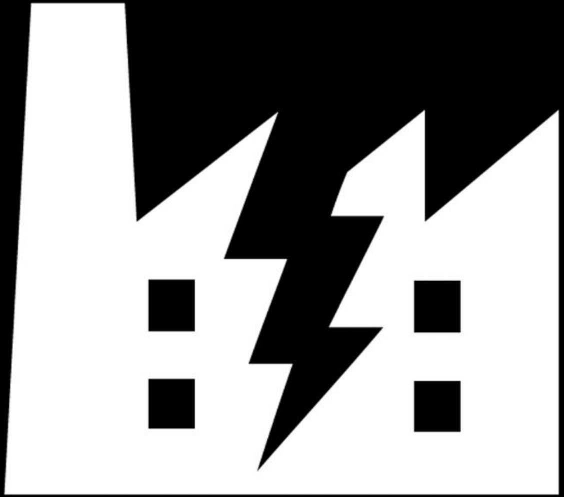
by Kristy Kepley-Steward | Thursday, September 17th 2020



More than 120 education and third-sector organisations may have had their data compromised through the breach of Blackbaud's cloud platform

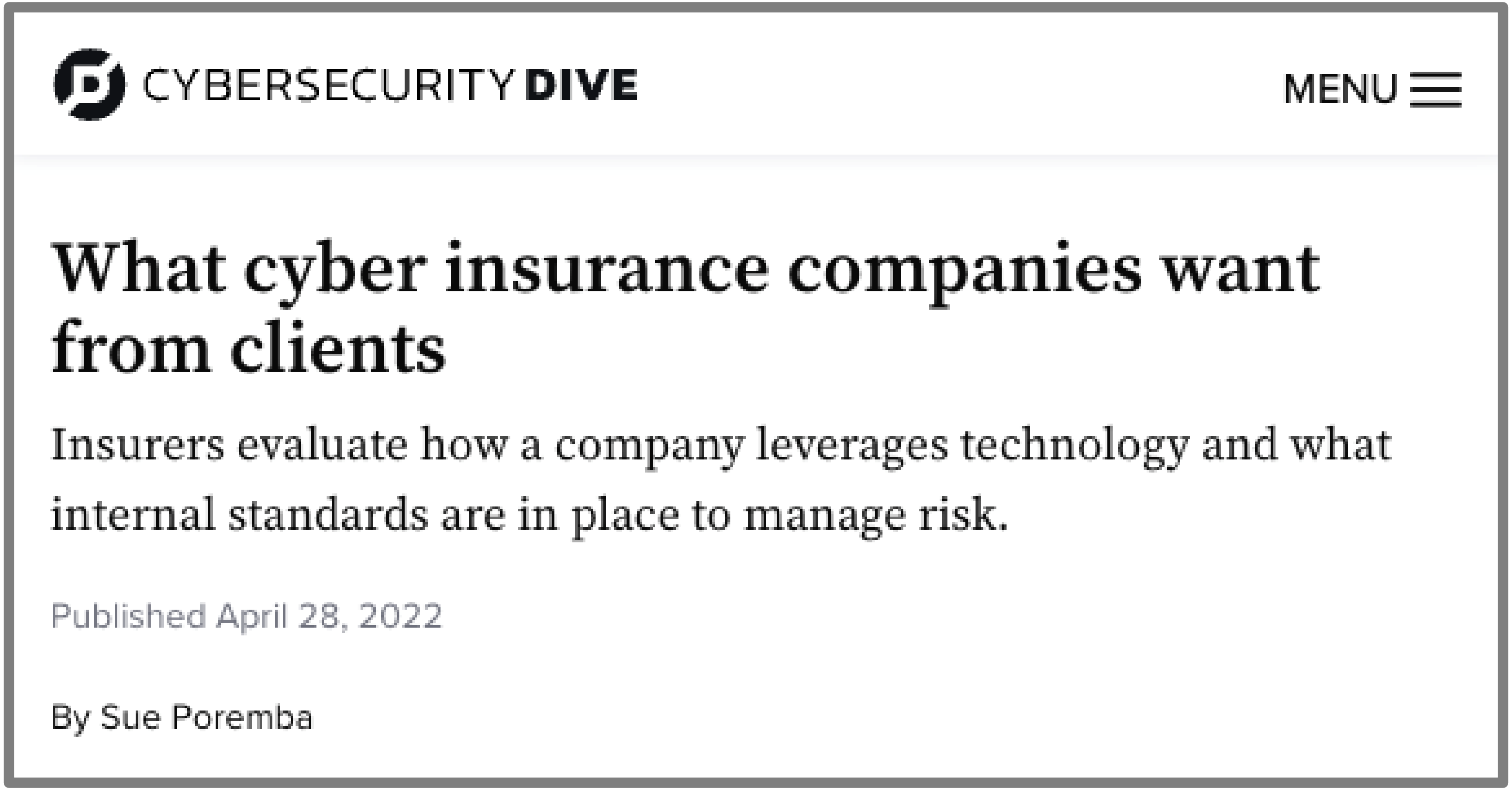
By Alex Scroxton, Security Editor

Published: 30 Jul 2020 9:06



INDUSTROYER2

Cyberattacks against Ukraine



What cyber insurance companies want from clients

Insurers evaluate how a company leverages technology and what internal standards are in place to manage risk.

Published April 28, 2022

By Sue Poremba

PREDICTIONS

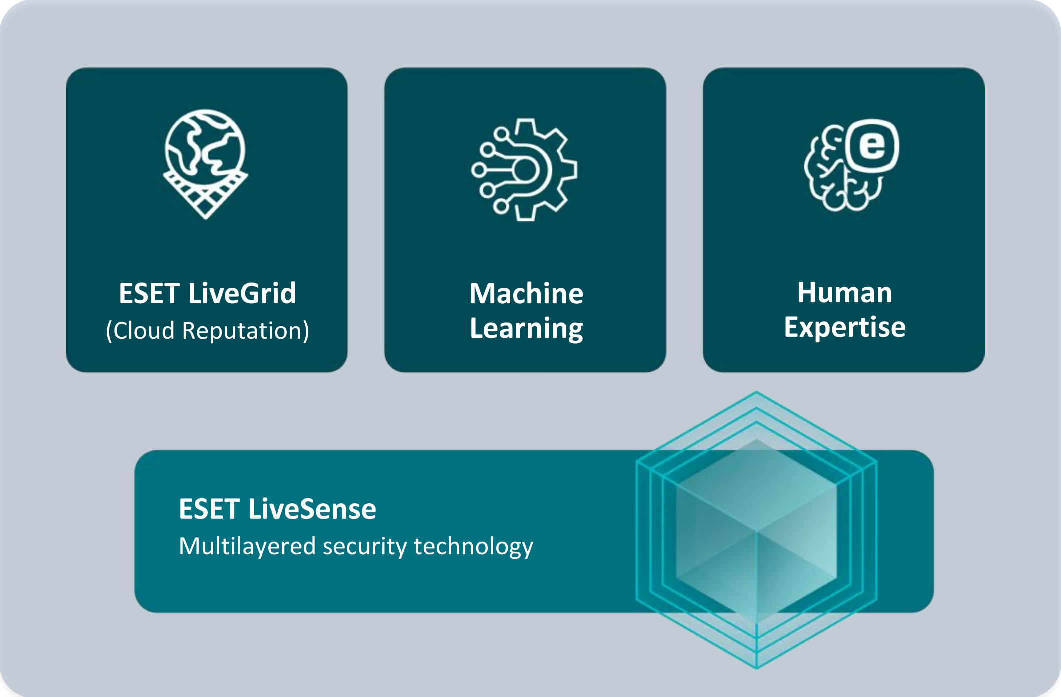
Are they connected?

How does this impact you?

Digital Security

Progress. Protected.

The ESET approach to cybersecurity



ESET LiveGrid
(Cloud Reputation)

Machine Learning

Human Expertise

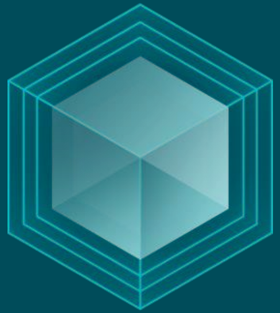
ESET LiveSense
Multilayered security technology

ESET LiveSense

A single layer of defense is not enough in today's constantly evolving threat landscape. ESET uses unique multilayered technologies that go far beyond the capabilities of basic antivirus.

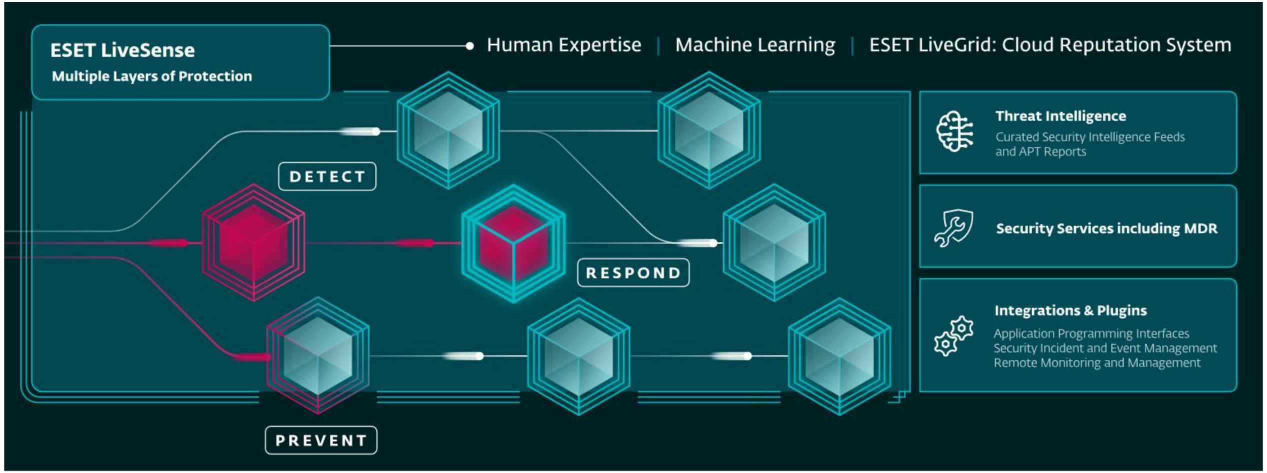
Sensors & Protection Layers

Botnet Protection	Secure Browser	Brute-Force Attack Protection	Exploit Blocker
Reputation & Cache	Network Attack Protection	DNA Detections	UEFI Scanner
Device Control	Ransomware Shield	Advanced Memory Scanner	Script Scanner & AMSI
Deep Behavioral Inspection	In-Product Sandbox	Advanced Machine Learning	Cloud Malware Protection System



ESET PROTECT Platform

A **unified cybersecurity platform** that integrates balanced breach prevention, detection and response capabilities, complemented by ESET managed & professional services, and threat intelligence. It is simple, modular, adaptable, and continuously innovated – always with the benefit of ESET customers in mind.



ESET LiveSense
Multiple Layers of Protection

Human Expertise | Machine Learning | ESET LiveGrid: Cloud Reputation System

DETECT

RESPOND

PREVENT

Threat Intelligence
Curated Security Intelligence Feeds and APT Reports

Security Services including MDR

Integrations & Plugins
Application Programming Interfaces
Security Incident and Event Management
Remote Monitoring and Management

Security Management ESET PROTECT

Detection & Response ESET Inspect

Advanced Threat Defense ESET LiveGuard

Modern Endpoint Security

Cloud Applications Protection

Encryption

Multi-Factor Authentication

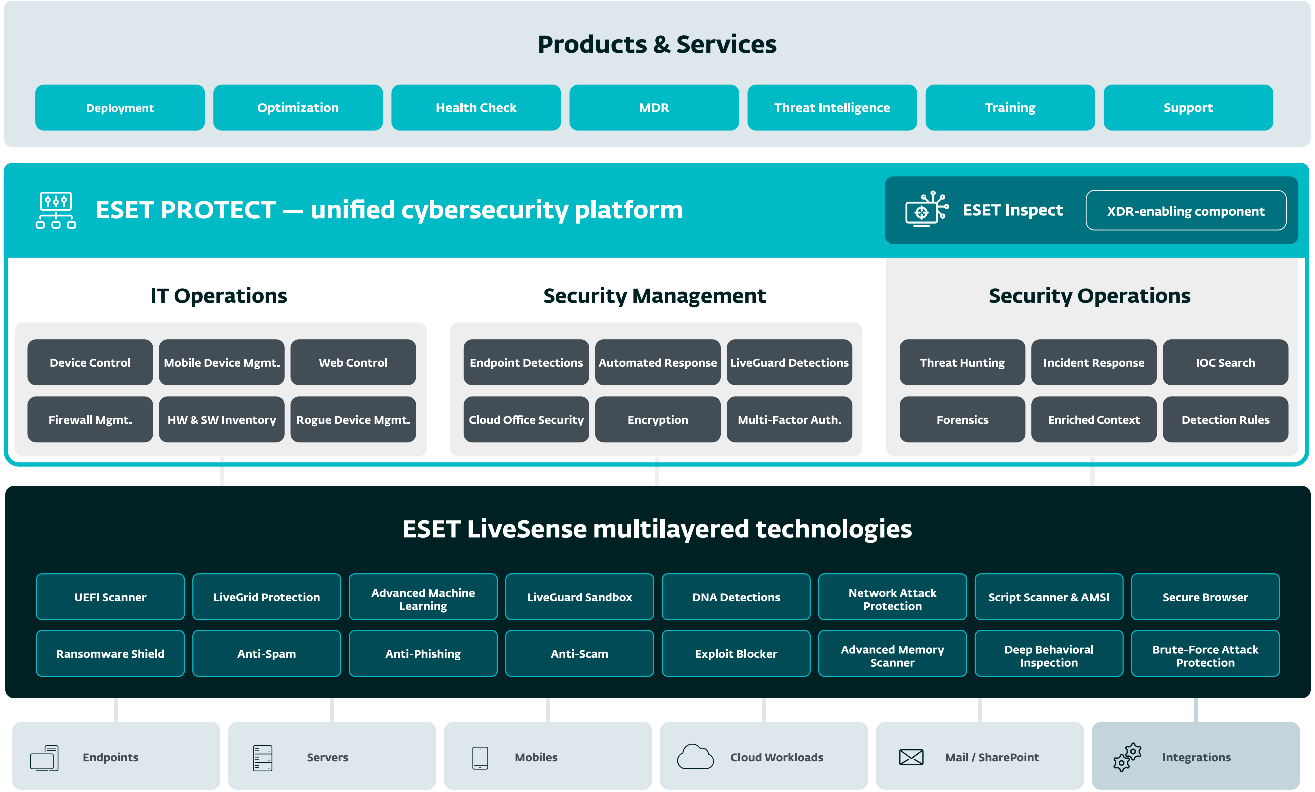
Mail Security

XDR capable

Internal educational slide deck for ESET HQ, Offices and Partners

XDR

ESET PROTECT Platform provides superior network visibility and extended detection and response (**XDR**) capabilities thanks to sophisticated tools like ESET Inspect.



Products & Services

Deployment | Optimization | Health Check | MDR | Threat Intelligence | Training | Support

ESET PROTECT — unified cybersecurity platform

ESET Inspect — XDR-enabling component

IT Operations

Device Control | Mobile Device Mgmt. | Web Control
Firewall Mgmt. | HW & SW Inventory | Rogue Device Mgmt.

Security Management

Endpoint Detections | Automated Response | LiveGuard Detections
Cloud Office Security | Encryption | Multi-Factor Auth.

Security Operations

Threat Hunting | Incident Response | IOC Search
Forensics | Enriched Context | Detection Rules

ESET LiveSense multilayered technologies

UEFI Scanner | LiveGrid Protection | Advanced Machine Learning | LiveGuard Sandbox | DNA Detections | Network Attack Protection | Script Scanner & AMSI | Secure Browser
Ransomware Shield | Anti-Spam | Anti-Phishing | Anti-Scam | Exploit Blocker | Advanced Memory Scanner | Deep Behavioral Inspection | Brute-Force Attack Protection

Endpoints | Servers | Mobiles | Cloud Workloads | Mail / SharePoint | Integrations

Internal educational slide deck for
ESET HQ, Offices and Partners

Full story

Everything we do is for a reason.

Just as no civilized, science-based society can thrive without modern medicine, so **no modern business can succeed without an effective response** in the face of an IT breach.

But given the pressures of modern life, and the lifestyle ailments that come with it, modern societies – like modern technology – are coming to realize that **surgery should not be our first response**.

As the philosopher Erasmus pointed out more than 500 years ago: **“Prevention is better than cure.”**

We believe in balance.

That’s why ESET has continued to invest heavily, over **more than 30 years**, in **multiple layers** of proprietary technology that **prevent** breaches of its customers’ endpoints and systems by both known and never-before-seen threats.

Occasionally, of course, prevention layers are breached – at which point, ESET sensors **detect** any intrusion and our automated **response** systems act immediately to intercept the threat and prevent it from causing damage.

This **extended detection and response (XDR)** solution, like modern surgical intervention, is an essential tool. But, like vaccines, **prevention technology does most of the heavy lifting** when it comes to avoiding harm – and ESET’s prevention technology is the most densely multilayered and effective in the industry, as proven in multiple tests.

Our understanding of Prevent, Detect and Respond

PREVENT

is the wealth of layered ESET protection technology that blocks malicious code or malicious actors from entering, or damaging, a user's system. The results from prevention are analyzed and used to further harden systems in order to repel future attacks.

EXAMPLE | **ESET Endpoint Protection**

DETECT

is the diagnostic and investigative technology that identifies post-execution malicious code based on its behavior, and triggers a response to prevent or mitigate damage. When a threat is identified and eliminated immediately, detection and response acts, in effect, as prevention.

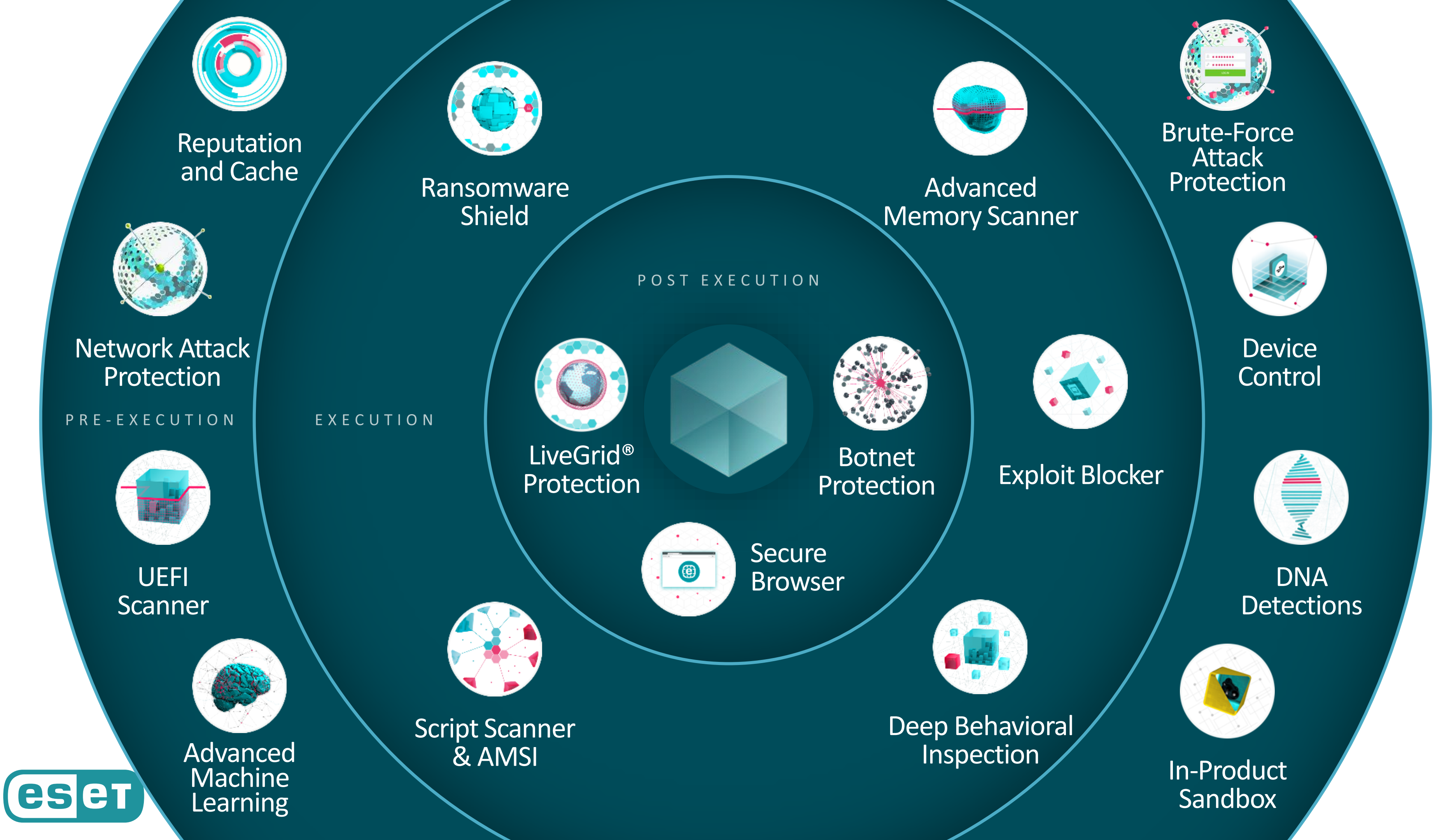
EXAMPLES | **ESET Inspect, ESET LiveGuard Advanced**

RESPOND

is the suite of automated and sometimes manual actions that halt, isolate, remove and/or mitigate a threat in order to prevent it spreading or doing significant harm. Response may also trigger automated notifications and forensic data collection that can be used to inform future prevention.

EXAMPLES | ESET cloud tech like **ESET LiveGrid**, modules like **ESET LiveGuard Advanced,** also **ESET Inspect**

SECRET
SAUCE
LiveSense
ESET



PRE-EXECUTION

Reputation and Cache

Network Attack Protection

UEFI Scanner

Advanced Machine Learning

Brute-Force Attack Protection

Device Control

DNA Detections

In-Product Sandbox

EXECUTION

Ransomware Shield

Advanced Memory Scanner

Exploit Blocker

Script Scanner & AMSI

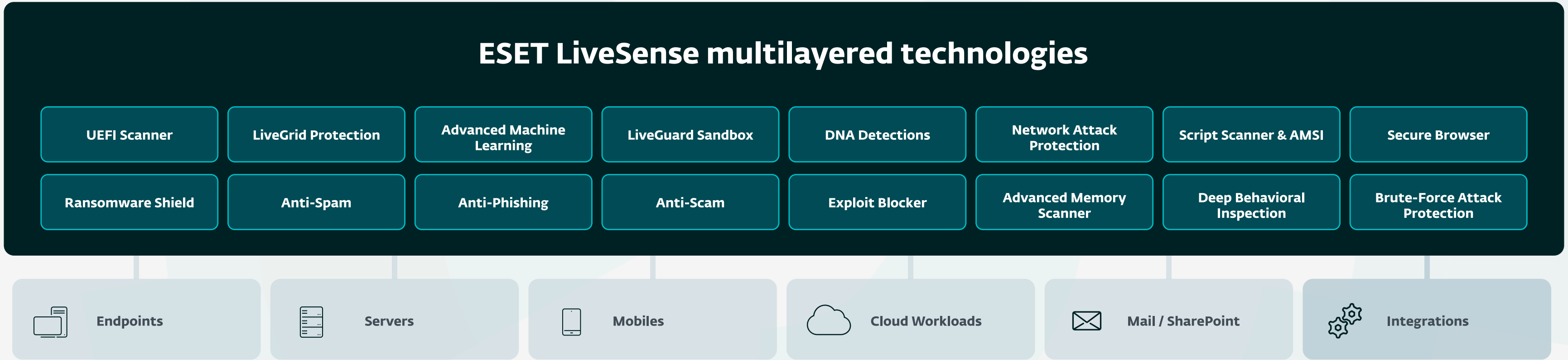
Deep Behavioral Inspection

POST EXECUTION

LiveGrid® Protection

Botnet Protection

Secure Browser



ESET LiveSense multilayered technologies

UEFI Scanner

LiveGrid Protection

Advanced Machine Learning

LiveGuard Sandbox

DNA Detections

Network Attack Protection

Script Scanner & AMSI

Secure Browser

Ransomware Shield

Anti-Spam

Anti-Phishing

Anti-Scam

Exploit Blocker

Advanced Memory Scanner

Deep Behavioral Inspection

Brute-Force Attack Protection

Endpoints

Servers

Mobiles

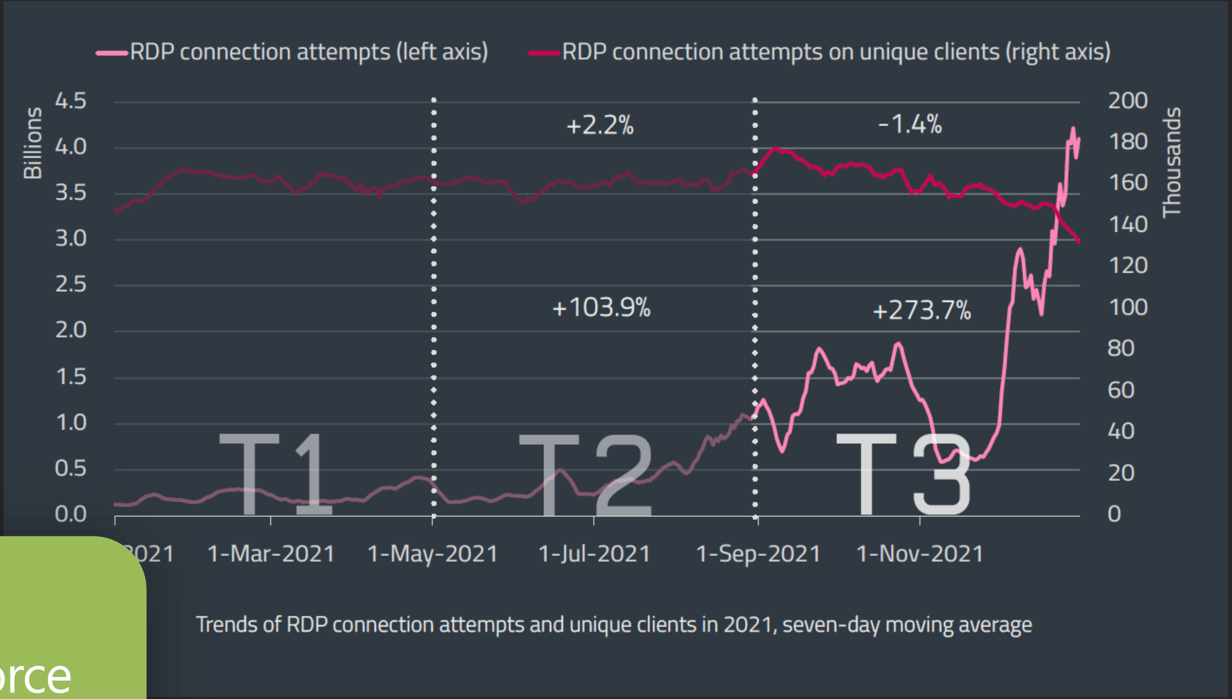
Cloud Workloads

Mail / SharePoint

Integrations

Brute-force attacks on RDP

In 2021 **increased by 900%**



Trends of RDP connection attempts and unique clients in 2021, seven-day moving average

ESET Brute-Force Attack Protection

ENJOY SAFER TECHNOLOGY™

Source: *welivesecurity.com – Threat report T3 2021*

ESET LiveSense

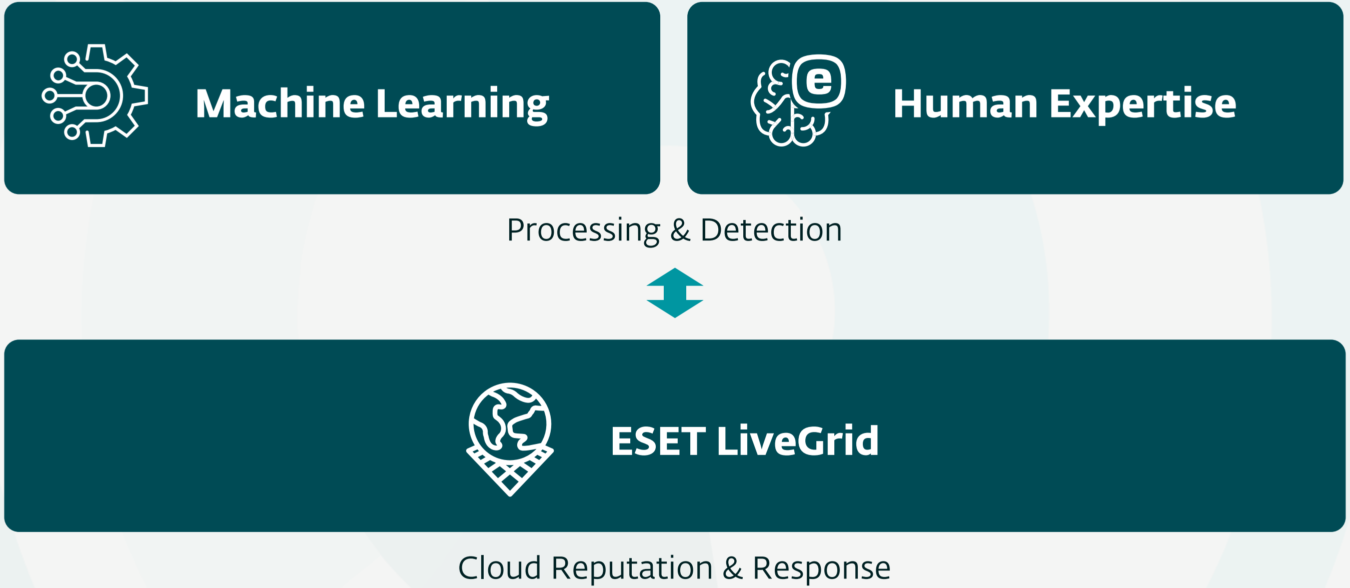
MULTILAYERED SECURITY TECHNOLOGY

MACHINE LEARNING

ESET LiveGrid®

HUMAN EXPERTISE

ESET APPROACH TO CYBERSECURITY



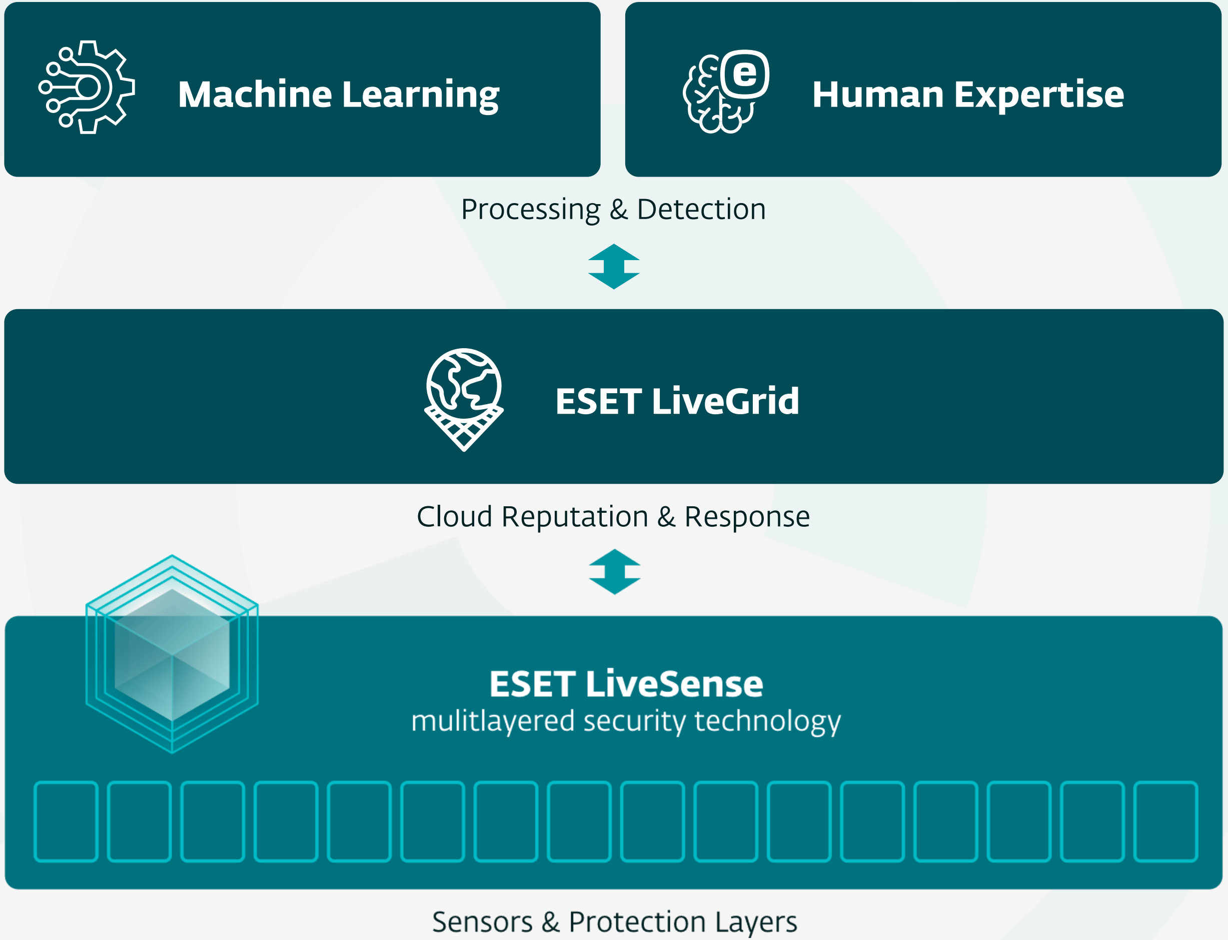
Machine Learning

Human Expertise

Processing & Detection

ESET LiveGrid

Cloud Reputation & Response



Machine Learning

Human Expertise

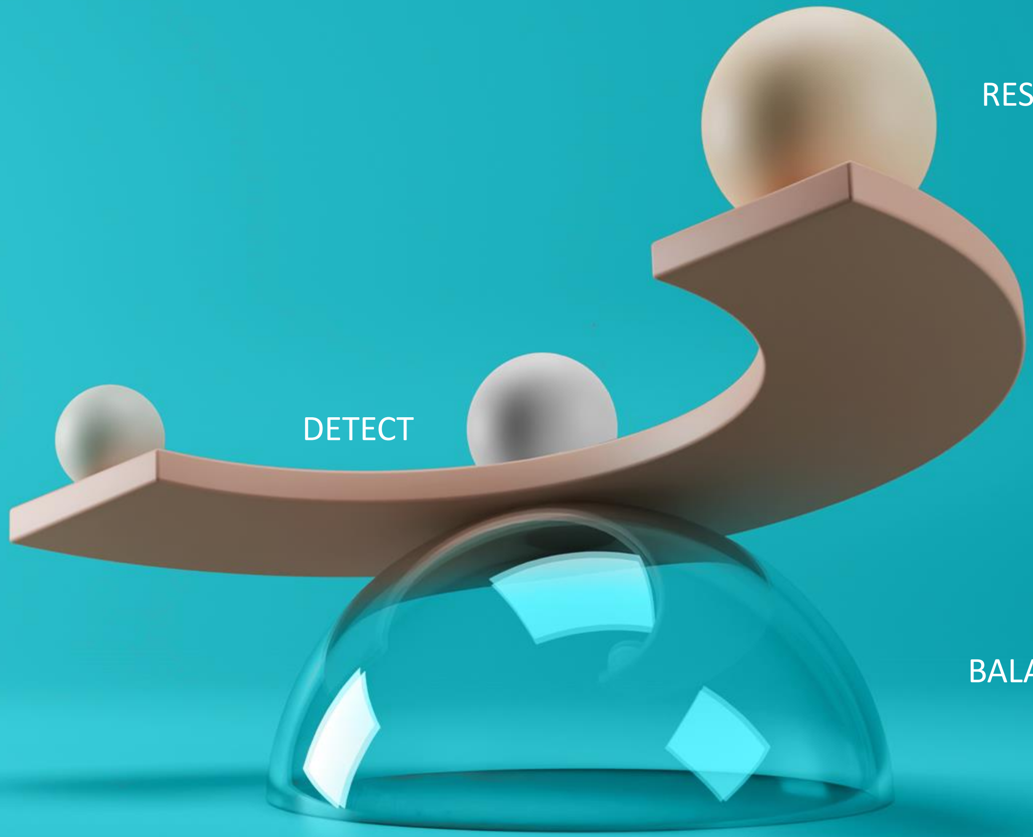
Processing & Detection

ESET LiveGrid

Cloud Reputation & Response

ESET LiveSense
mulitlayered security technology

Sensors & Protection Layers

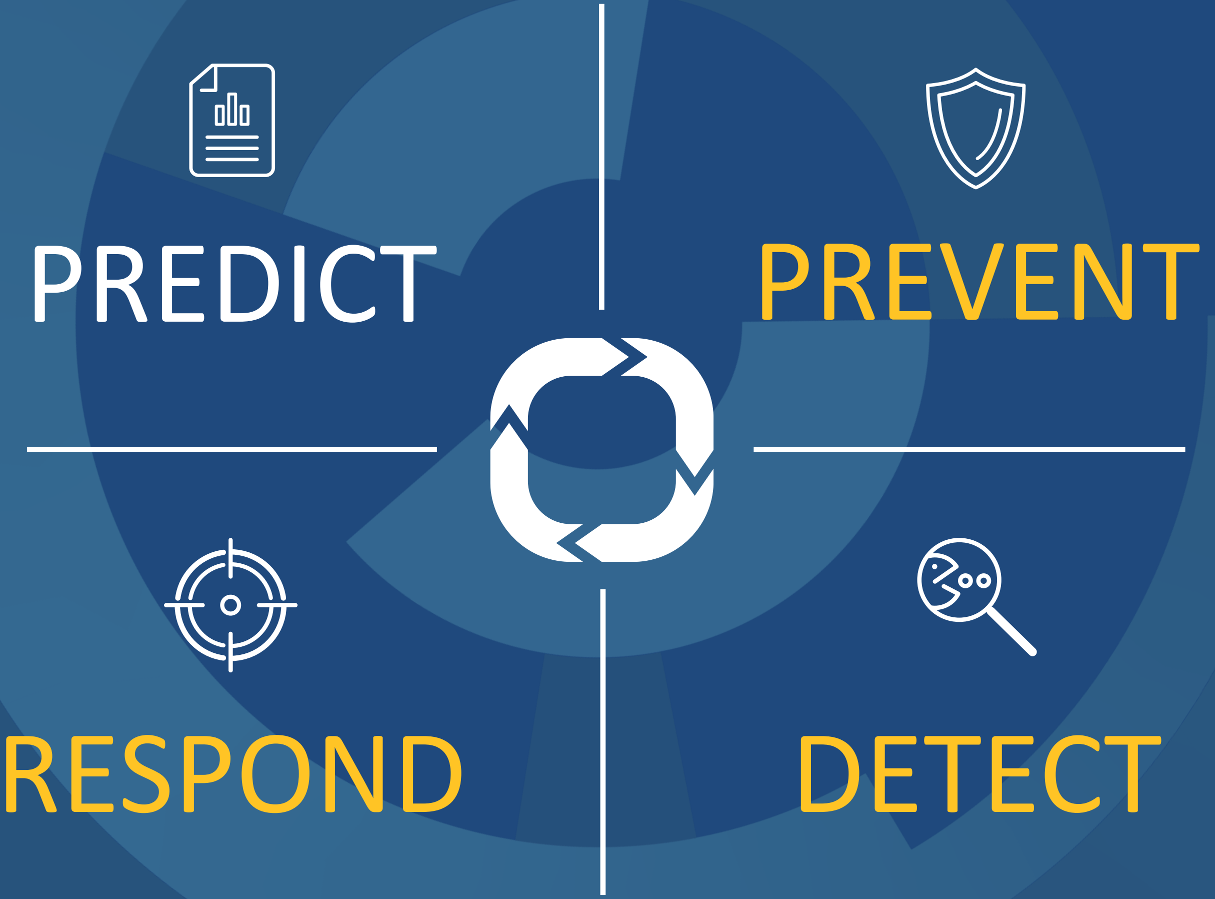


RESPOND

PREVENT

DETECT

BALANCE



PREDICT

PREVENT

RESPOND

DETECT

ESET

PREVENT

DETECT

RESPOND

Call to Action

Think about your cyber security posture

Think about sources of threat intelligence

Consult with ESET

Crisis scenario

Advanced Memory Scanner

Exploit Blocker

Close ports

Monitor for suspicious behaviour

2FA

Secure passwords

Ransomware Shield

Test backups

Third-party supply chain

Awareness training

Anti-malware

Update and patch

Continuity plan

Audit user access

ESET Dynamic Threat Defense

THANK YOU