NetCo TECHNOLOGY

IT KLINIKA RELOADED

THE BREACH

Napadač ima pristup unutar sistema, kreće borba: EDR, XDR, detekcija i reagovanje, zašto je brzina reakcije presudna?

Dimitrije Veličanin

ENDPOINT SECURITY

Top Security Pros Know

Despite massive investments in cybersecurity platforms, risk continues to rise

35% increase in cloud breaches	**$4.4M** average cost of a breach
50% increase in cyber insurance premiums	**3/4** boards fear a major cyber attack in next 12 mos

Vendors have created a

False Sense of Comfort

NetTECHNOLOGY

ENDPOINT SECURITY

Key Security Use Cases

COMPLIANCE REQUIREMENTS PRESENT MATERIAL RISK

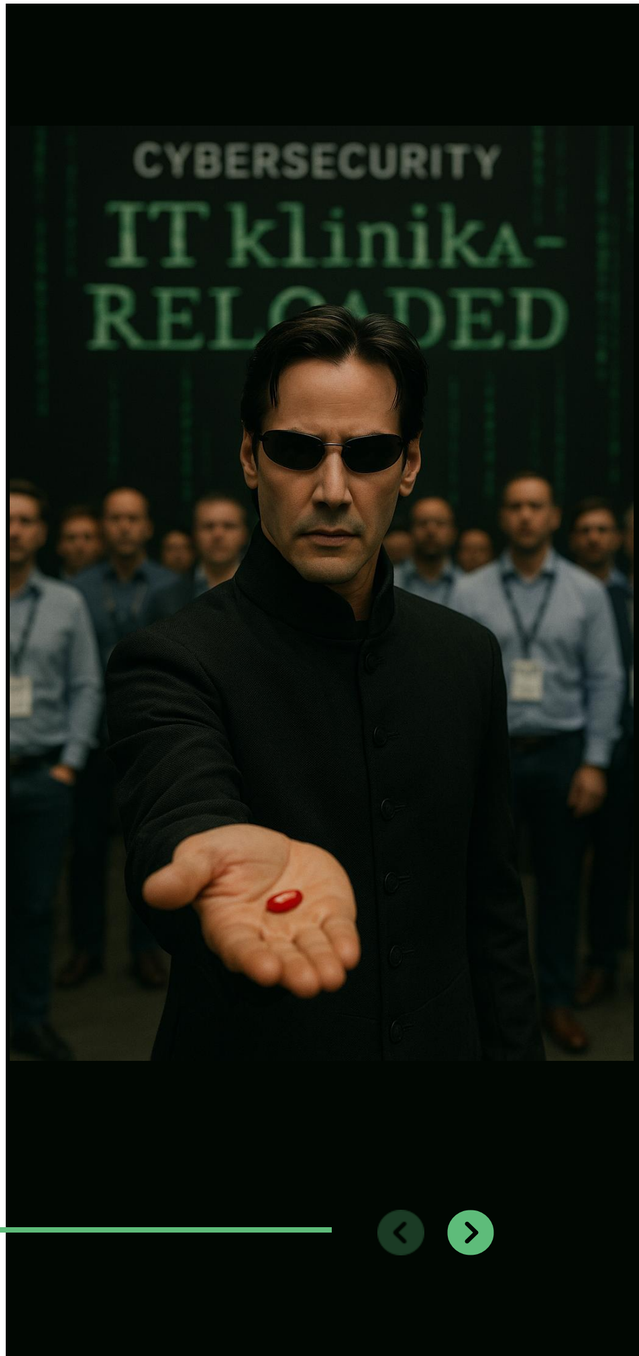
- Large organizations must adhere to numerous compliance regulations
- Enterprise data is spread across private networks and in the cloud
- **Symantec Endpoint Security** enables compliance controls to be applied and managed consistently across the infrastructure

SAFELY ENABLING A REMOTE WORKFORCE

- “Disappearing perimeter”
- Sensitive enterprise apps and data are everywhere
- **Symantec Endpoint Security** enables users to securely access the assets they have rights to, from anywhere

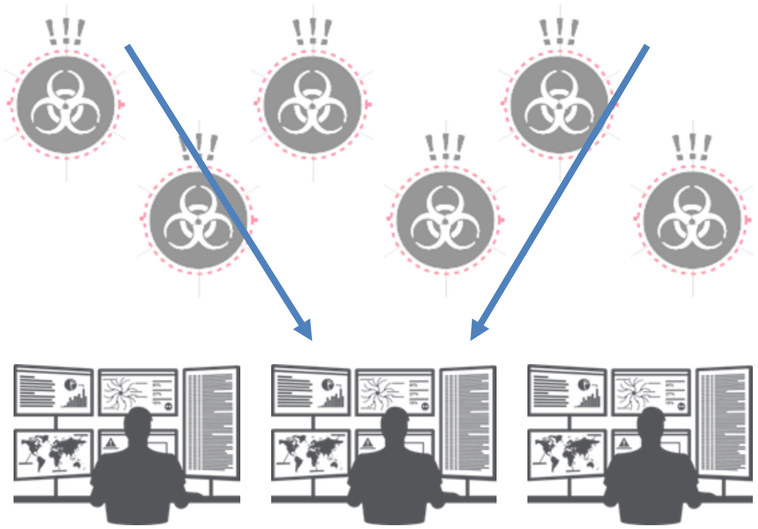
A NEW GENERATION OF ATTACKS TARGETING ENTERPRISES

- Targeted ransomware
- Supply Chain attacks
- **Symantec Endpoint Security** unifies security and telemetry across control points to stop new attacks on devices, networks, e-mail, and in the cloud



ENDPOINT SECURITY

Gram prevencije vredi više nego kilogram detekcije i odgovora na pretnje (detection and response)

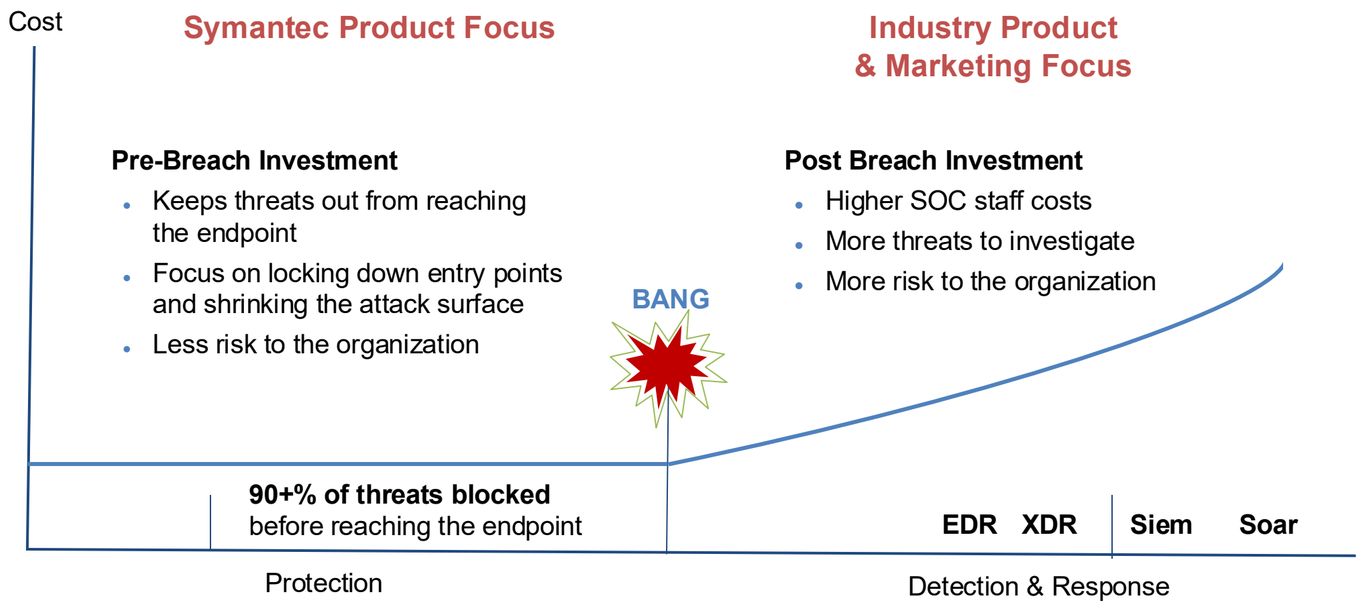


- Without good prevention, more attacks get through
- Reactive security programs place a greater burden on the SOC
- Incident response is expensive; strong prevention helps reduce costs and workload
- Rich prevention metadata provides enhanced Threat Intel for the SOC

NetPlus TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Endpoint Security | Market Approach



Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Symantec
Endpoint Security Complete

Industry-best protection across all devices and OSes

Windows, Mac, Linux, iOS, Android, Windows 10S/11S

- Endpoint Protection (evolution of SEP)
- Endpoint Detection & Response
- Threat Hunter & Threat Intelligence
- Adaptive Protection
- Application Control
- Threat Defense for Active Directory
- Rich Public APIs for XDR Integration

Symantec™ by Broadcom

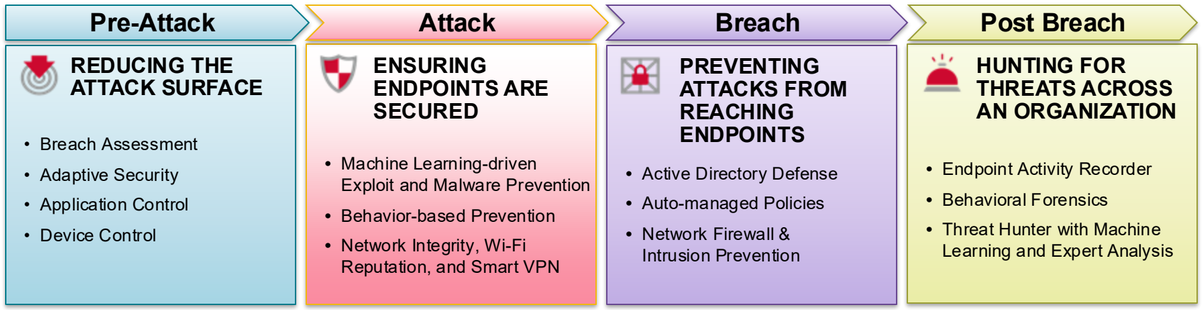
NetOne TECHNOLOGY

KAKO TO STVARNO IZGLEDA (DEMO)?

- Win+R malware - https://www.it-klinika.rs/blog/lazni-captcha-testovi - email-a za Slavicu sa linkom ka Win+R malware-u
- skripta koja se automatski kopira u Clipboard i pokreće CnC agenta
- opis Caldera alata za simulaciju i osnovne funkcije
- Slavica otvara email sa linkom preko zasticenog netpplab domena, i pokusava da se verifikuje
- Slavica ovara email sa nezasticenog domena i prati instrukcije
- pregled PA logova koji detektuju ovaj saobracaj
- prikaz agenta u Calderi i prikaz Adversary-a koji ce se koristiti nakon cega sledi pokretanje operacije napada:
  - Signed Binary Proxy Execution
  - Stowaway
- price o SESC tehnologijama sa osvrtom na Adaptive Protection
- pokazivanje reakcije SES agenta i pregled napada u Calderi
- pregled incidenata u SESC konzoli
- AI Generated Summary incidenta

SYMANTEC ENDPOINT SECURITY COMPLETE

SES Complete – Protection Across the Attack Chain



Adaptive Protection – Threat landscape insights, custom behavioral insights, and recommendations

Single Agent – all operating systems: Windows, Mac, Linux, Windows S Mode, Android, and iOS – including servers

Global Intelligence Network – World's largest civilian cyber intelligence network

Security Integrations – Enabling Symantec product and third-party integrations

Symantec™ by Broadcom

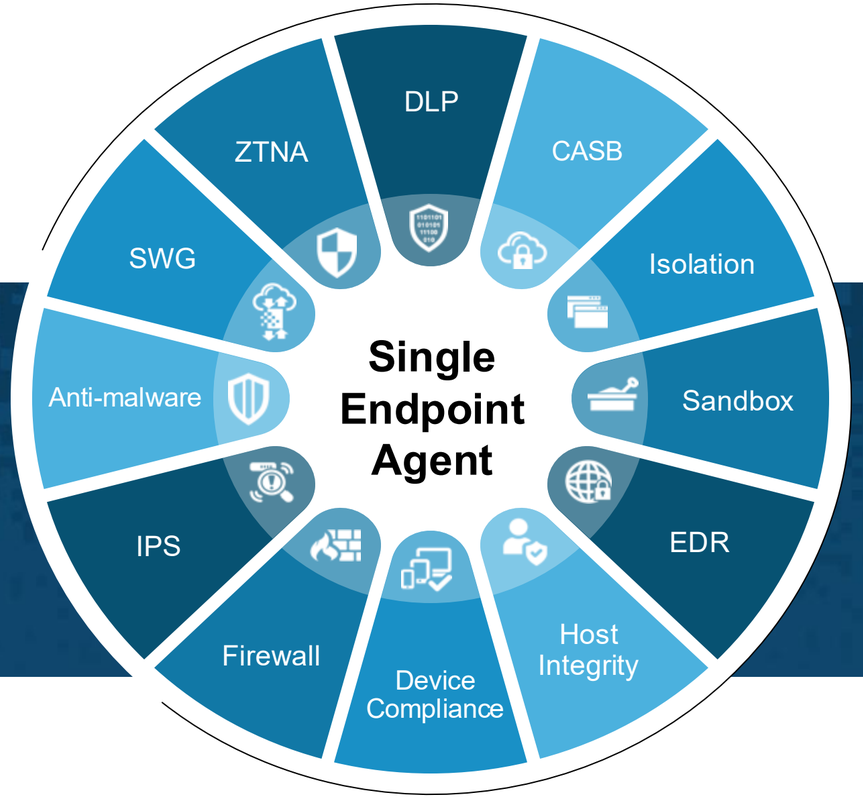
NetOO TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Innovation: Integrating to a Single Agent

Reduced operational overhead and a better user experience

- **Faster time to production**
- **Granular rollout of capabilities**
- **Reduced management overhead**



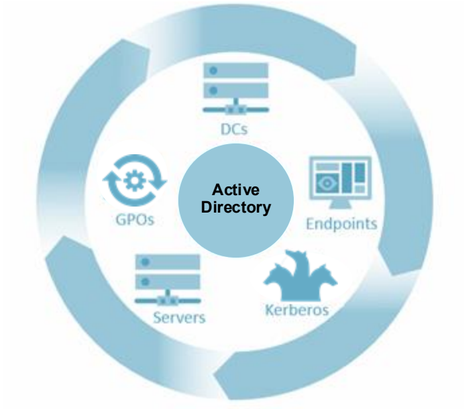
Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Attack Surface Reduction

Breach Assessment



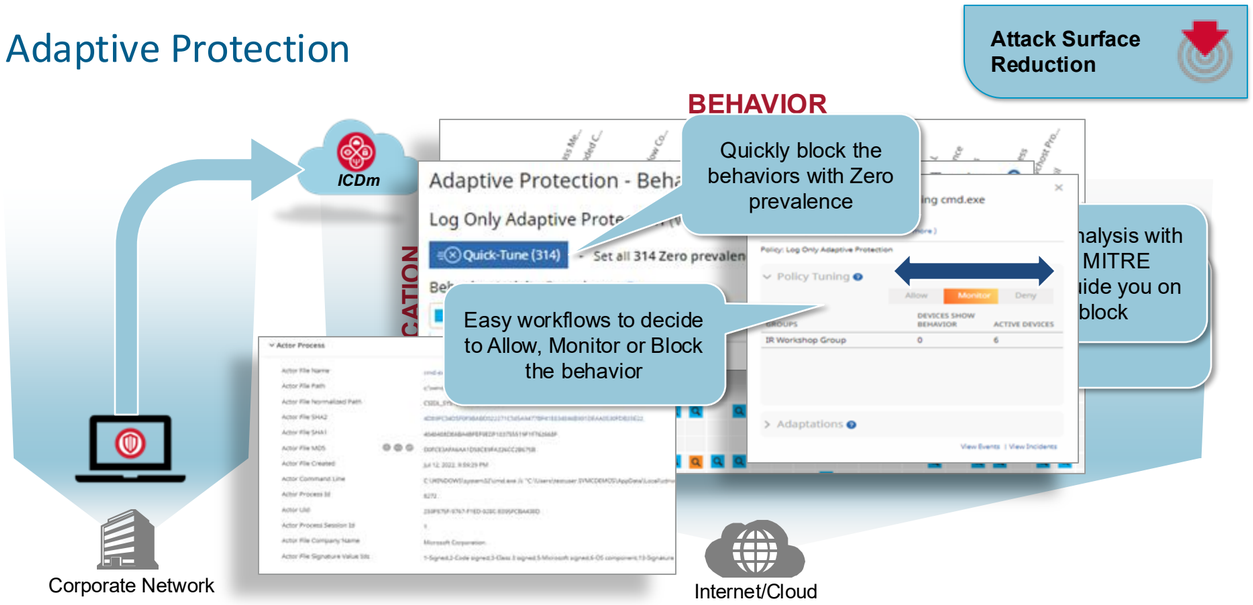
Symantec delivers proactive endpoint defense with pre-attack surface reduction capabilities

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Adaptive Protection



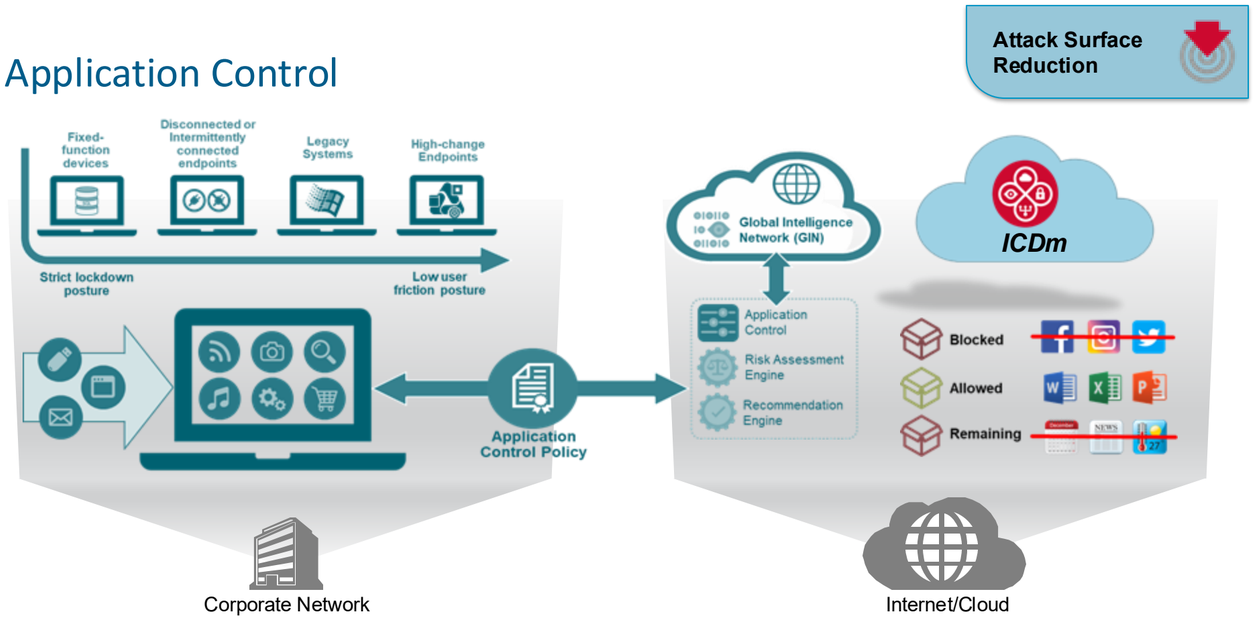
Adaptive Protection will do the work of identifying the use of LOTL tools in your organization for you

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Application Control

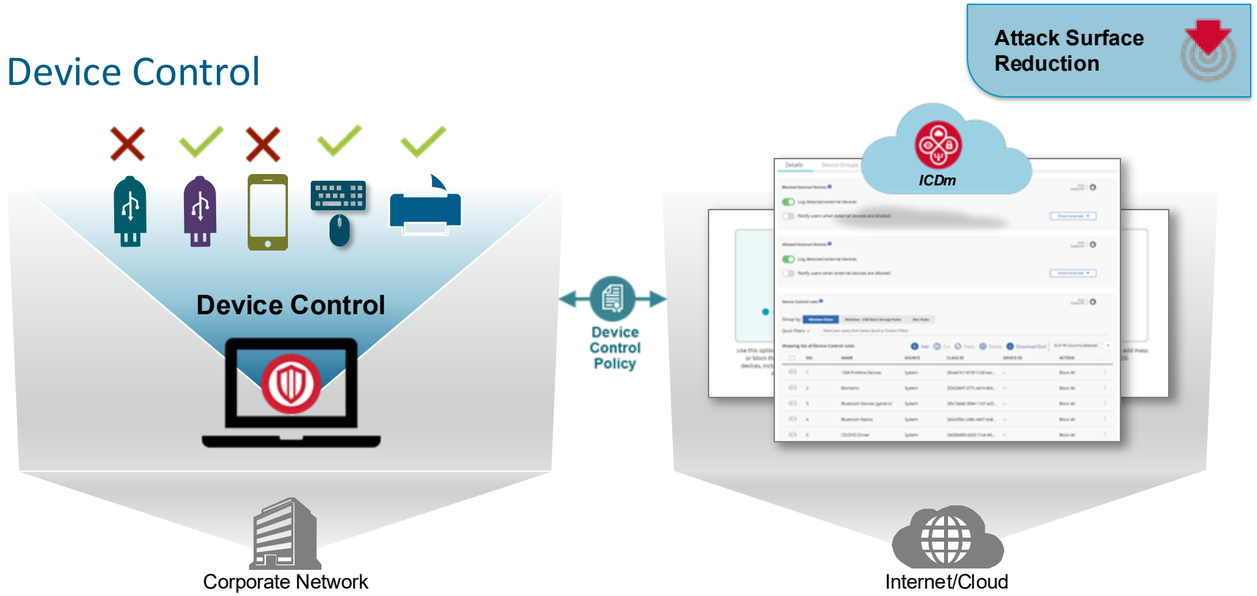


Assesses the risk of applications and allows only known good applications to run

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE



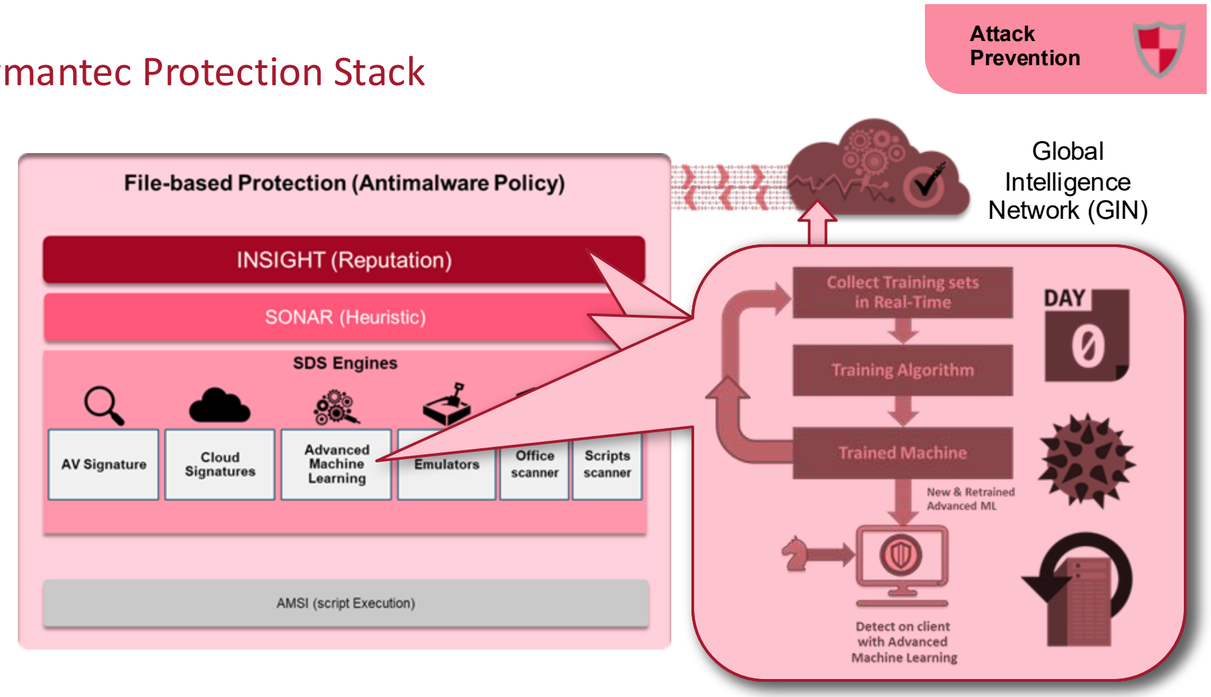
Reduces the risk of threats and exfiltration from devices on Windows and Mac operating systems

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Symantec Protection Stack



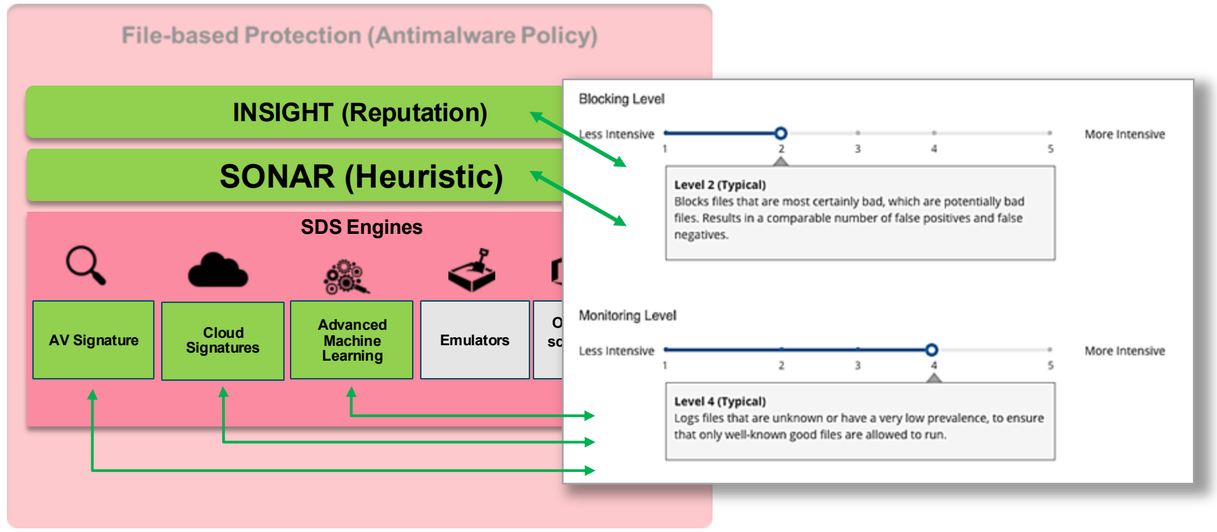
Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Symantec Protection Stack

Attack Prevention



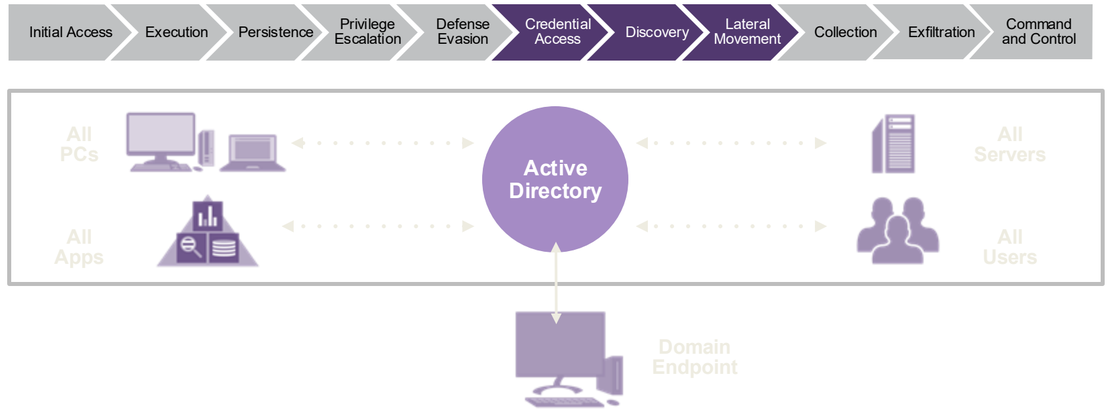
Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Active Directory Defense

Breach Prevention



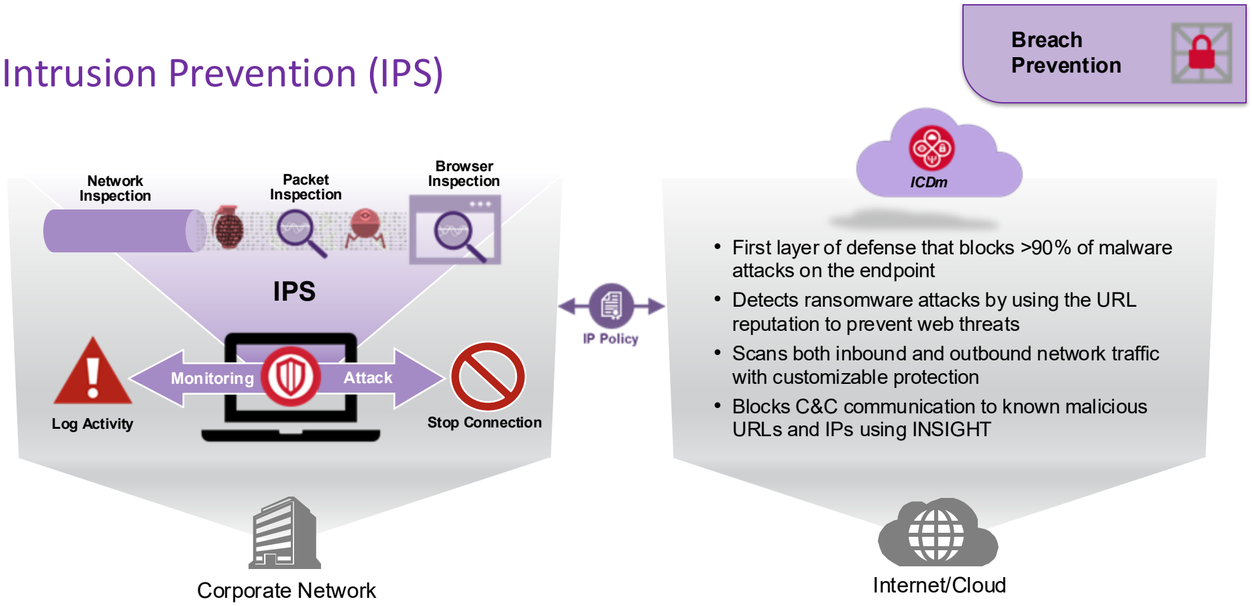
With a few queries to active directory at the breached endpoint, an attacker can obtain information about the corporation and move laterally

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Intrusion Prevention (IPS)



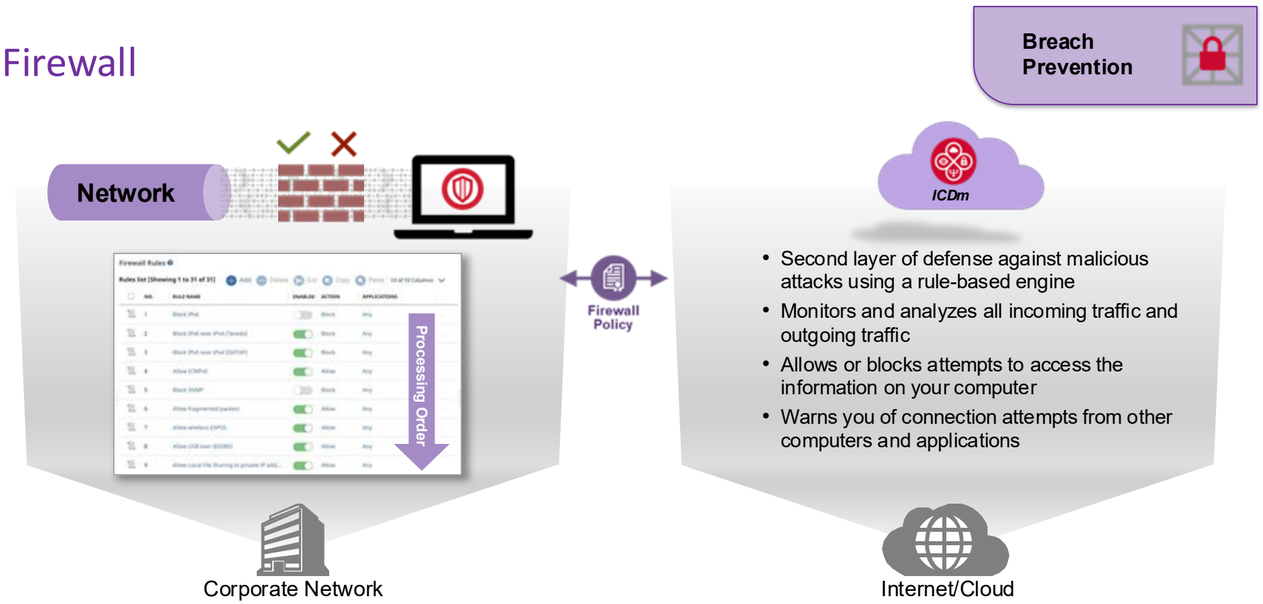
IPS runs at the packet level to inspect traffic for malicious communication patterns

Symantec by Broadcom

NetOO TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Firewall



The firewall inspects inbound and outbound traffic through a set of rules in the firewall policy

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Targeted Attack and Incident Response Challenges

Detection & Response

Threat actors are shifting their focus to large organizations where they can cause more **disruption** and demand **higher ransom** amounts.

191

Average days attackers dwell in a **customer environment**

53%

Of firms cite cyber security **skills shortage**

38%

Time SOC teams spend **fighting alerts**

Increased threats - decreased resources - complex environments - alerts from multiple sources.

Symantec™ by Broadcom

NetPlus TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Endpoint Detection & Response

Provides continual security improvement & proactive attack surface reduction in the environment

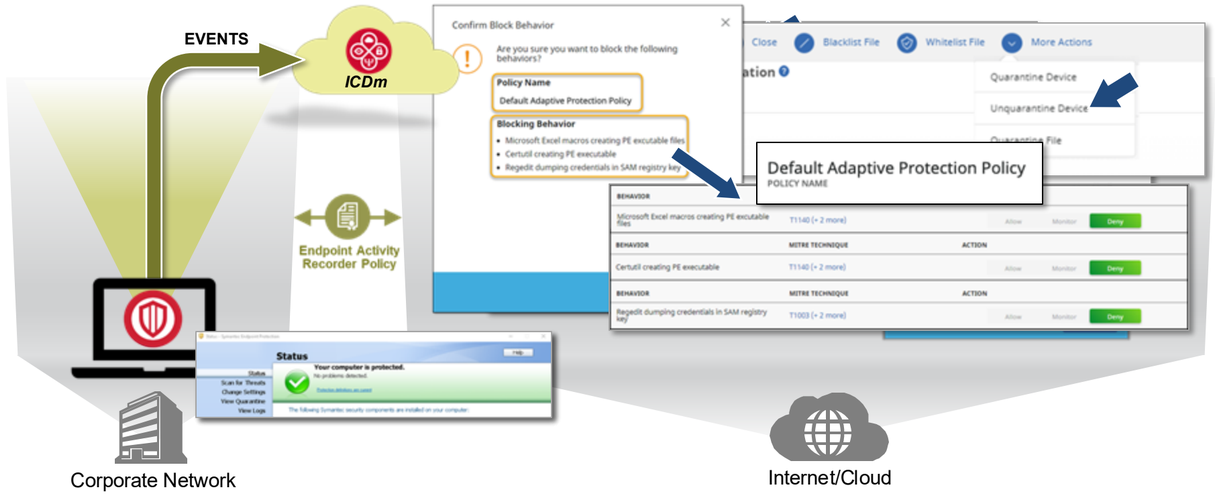
Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Endpoint Detection & Response

Detection & Response



Prevent the threat from spreading through the network now and in the future

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

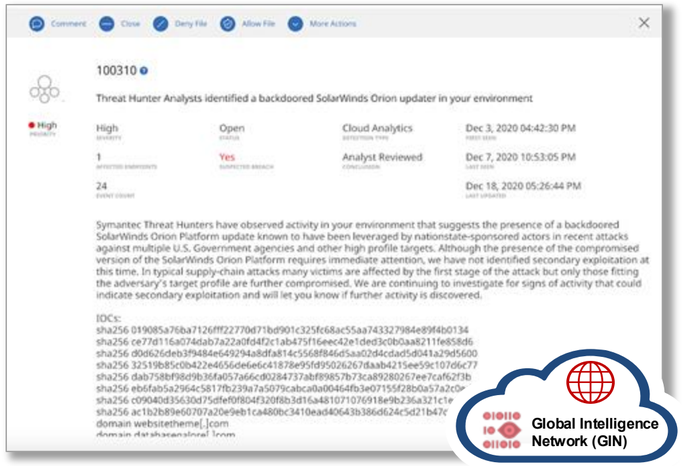
Threat Hunter Feature

Detection & Response

FIND TARGETED ATTACK ACTIVITY
Discover high-fidelity incidents using rich telemetry, machine learning & cloud analytics

RECEIVE INDICATORS FROM EXPERTS Gain detailed findings from Symantec Threat Expert Analysts including tactics, techniques, and procedures (TTPs) used by adversaries.

ACCESS FULL GLOBAL INTELLIGENCE
Identify attacks through intuitive access (+ via API) to Symantec's global security data



Symantec by Broadcom

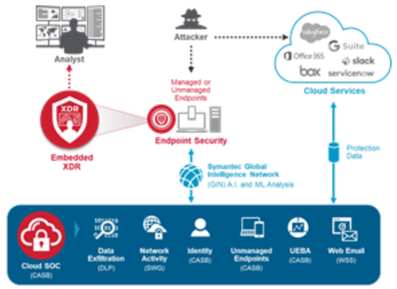
NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

SES Complete Product Integrations

Extended Detection & Response (XDR)

- Extended Detection & Response feature of SES Complete integrates with CloudSOC CASB
- CloudSOC events and incidents can be correlated with behaviors that are observed and identified as potential incidents in SESC
- Data is enriched with authoritative threat intelligence from the Symantec GIN
- XDR incidents are presented in a single, cloud-delivered console within SESC
- Out of the box operation without additional 3rd party integrations or services
- Covers both managed and unmanaged devices
- Provides context that helps analysts to more quickly and thoroughly investigate IOCs and understand related response actions



Web & Cloud Access Protection

- Web and Cloud Access Protection integration in SESC protects endpoints from unsafe URLs by redirecting network traffic to the Symantec Cloud Secure Web Gateway (Cloud SWG), where the Cloud SWG policies allow or block the traffic on the SES Agent.
- Integration with the Cloud SWG ensures that employees cannot access malicious websites or cannot adhere to your already defined web-use policies.
- The SES Agent handles all supported traffic in one of the following ways
  - Redirects it to the Cloud SWG server
  - Blocks it
  - Allows it to continue to its destination
- Requires a valid Cloud SWG subscription for use in SESC

Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

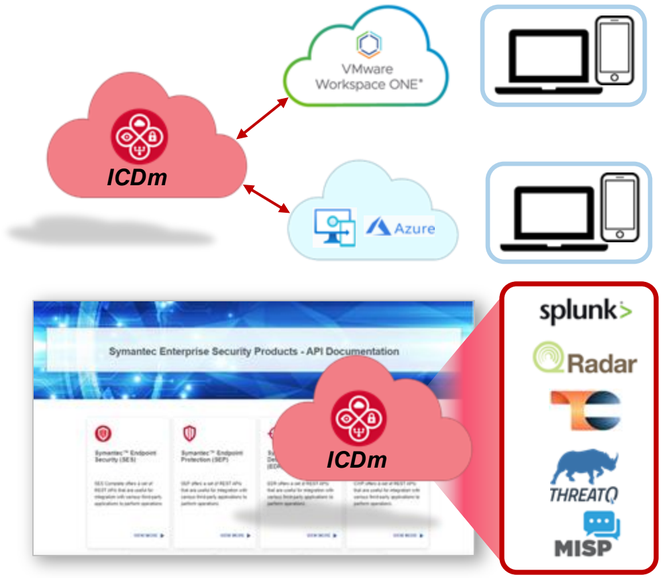
SES Complete Product Integrations

Unified Endpoint Management (UEM)

- Use **Unified Endpoint Management (UEM)** in SESC to configure your UEM provider (MS Intune/ VMware Workspace ONE) and discover your Windows, Android, and iOS devices
- After SESC establishes connections with your UEM, devices appear as unmanaged devices, can be enrolled and managed and will synchronize the applications that are found
- Integrating SES Complete with your organization's UEM is highly recommended as it allows:
  - A seamless and easy deployment of the Symantec Agent
  - Advanced security features and security enforcement.
  - The discovery of your Android and iOS devices

3rd Party / API Integrations

- Integrate with third-party products using the **Symantec Endpoint Security REST APIs**
- Stream or export events at real-time to a third-party Security Information and Event Management (SIEM) tools using the **Event Stream API**
- Integrate Broadcom Threat Intelligence TAXII feeds with **Splunk, QRadar, ThreatConnect, ThreatQ and MISP**
- Use **Cloud Platform Connections** to connect with cloud platforms (AWS/Azure) to discover and protect the instances or virtual machines, and their workloads.



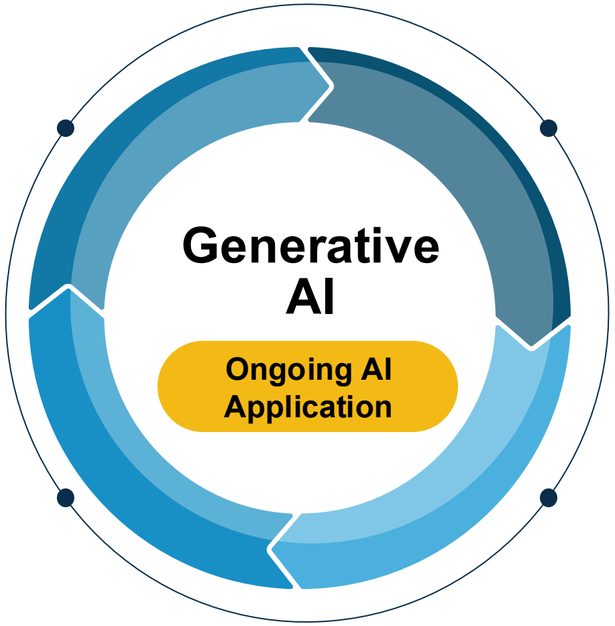
Symantec by Broadcom

NetOne TECHNOLOGY

SYMANTEC ENDPOINT SECURITY COMPLETE

Endpoint Platform Innovation | AI Integration
Delivered in Symantec Endpoint Security

Threat Descriptions
Faster analysis of unknown files submitted for threat investigations. Helps with analysis and provides descriptions and summaries.



Adaptive Protection & Isolation
Adaptive features in our protection and EDR stack use AI to map behaviors and patterns and make adaptive recommendations

Incident Summaries
AI generated incident summaries in EDR Cloud analytics make incident triage faster and easier

Chatbot
AI used to accelerate support and service.

Symantec™ by Broadcom

NetOne TECHNOLOGY

UMESTO

NetPP TECHNOLOGY

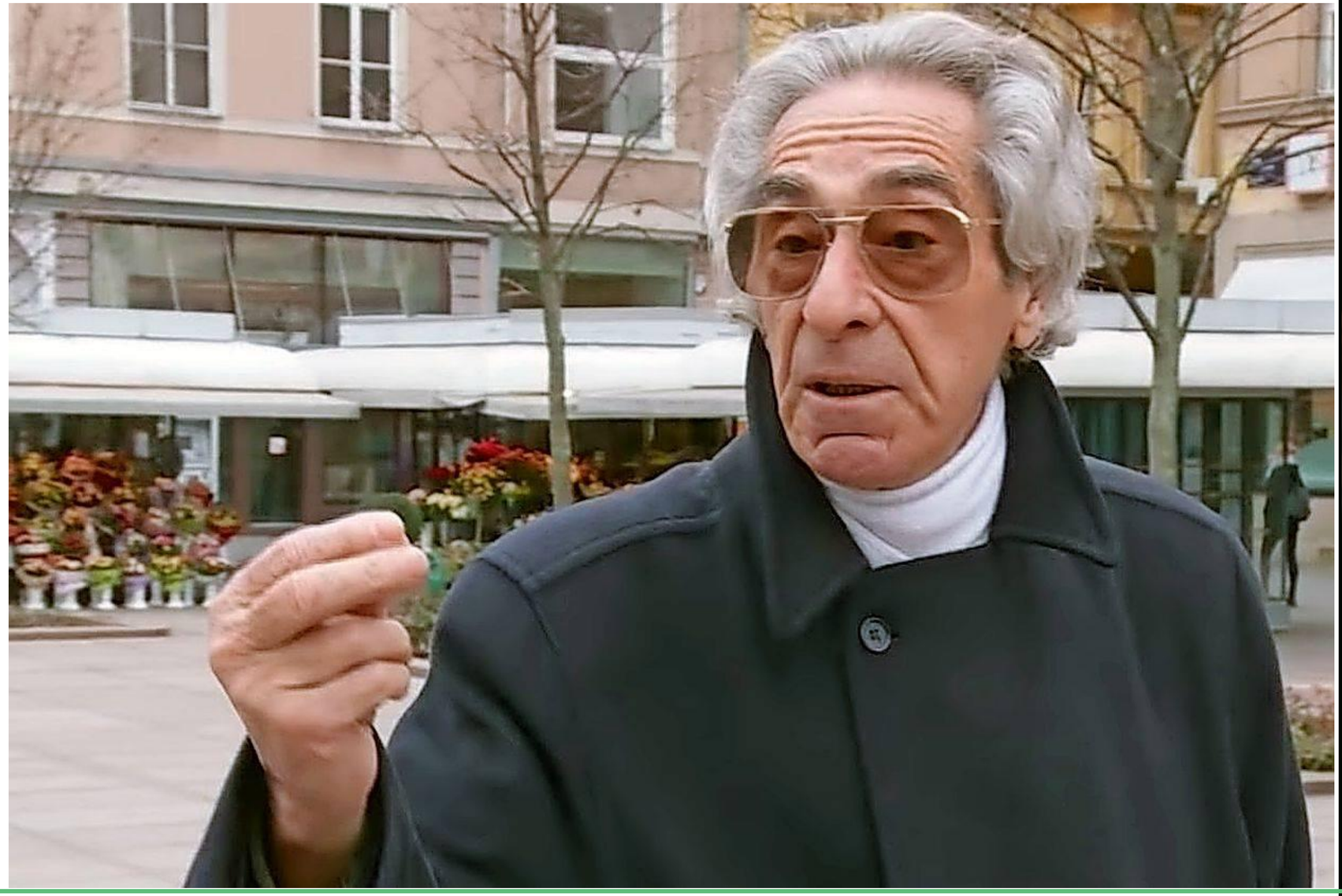
ZAJEDNO SA NAMA

NetPlus TECHNOLOGY

ZAJEDNO SA NAMA

NetPlus TECHNOLOGY

VEZBAJ!



NetPlus TECHNOLOGY

VEZBAJ!

Zašto BAS (Breach & Attack Simulation)?

Nije samo puka vežba u pitanju, koja ukazuje na stvarne slabosti, rupe u zaštiti, pogrešne konfiguracije već i:

- Proaktivno otkrivanje ranjivosti pre nego što ih napadači iskoriste
- Kontinualna validacija bezbednosnih kontrola, politika, planova, procedura
- Unapređenje IR i trening tima kroz realne situacije
- Povećanje otpornosti organizacije na nove pretnje

Prelazak sa reaktivnog na proaktivni model odbrane od sajber napada!

NetPlus TECHNOLOGY

PITANJA?

NetPlus TECHNOLOGY

HVALA NA PAŽNJI

+381 11 36999 967

www.netpp.rs

Otokara Keršovanija 11/39, Beograd