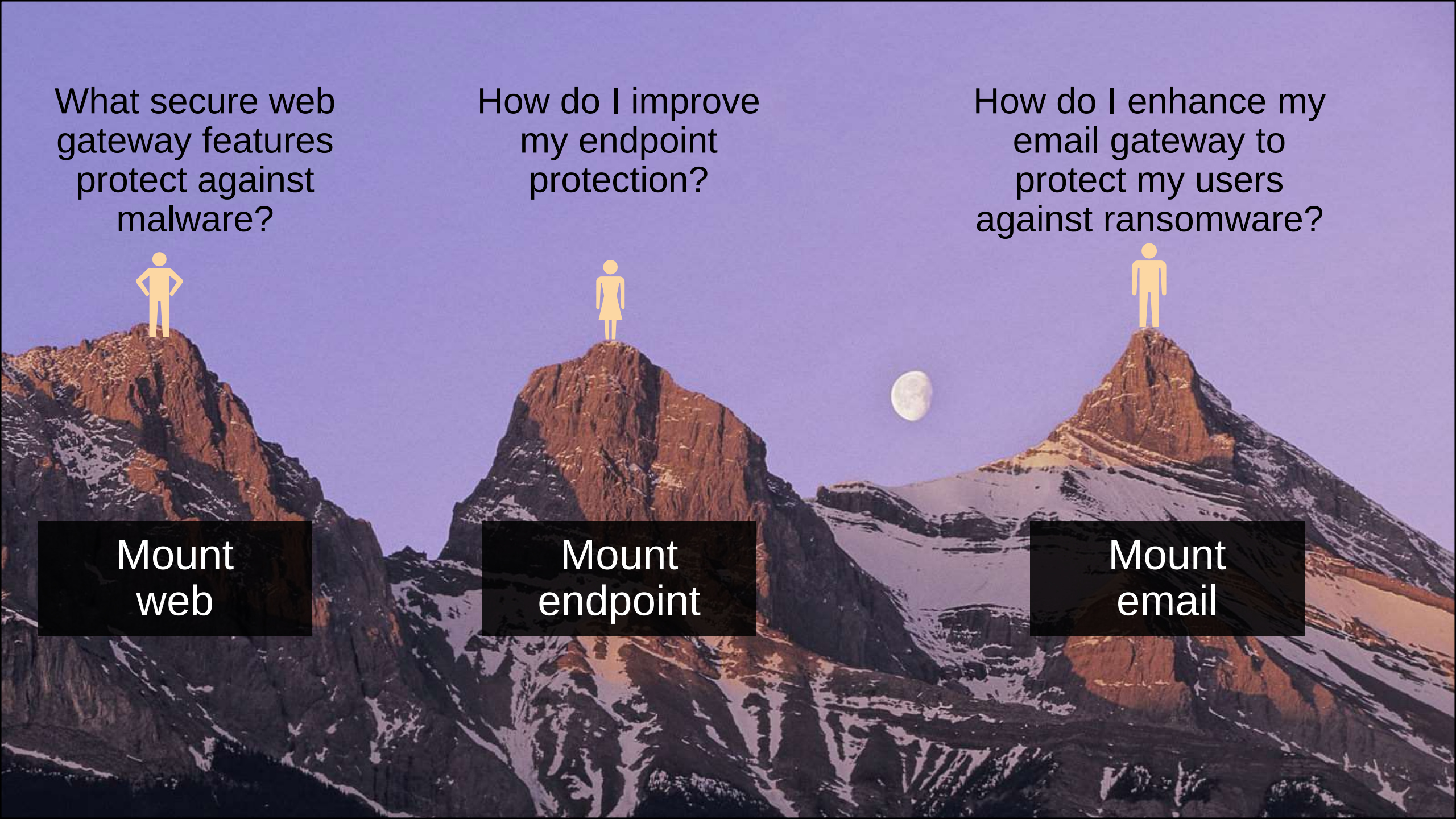
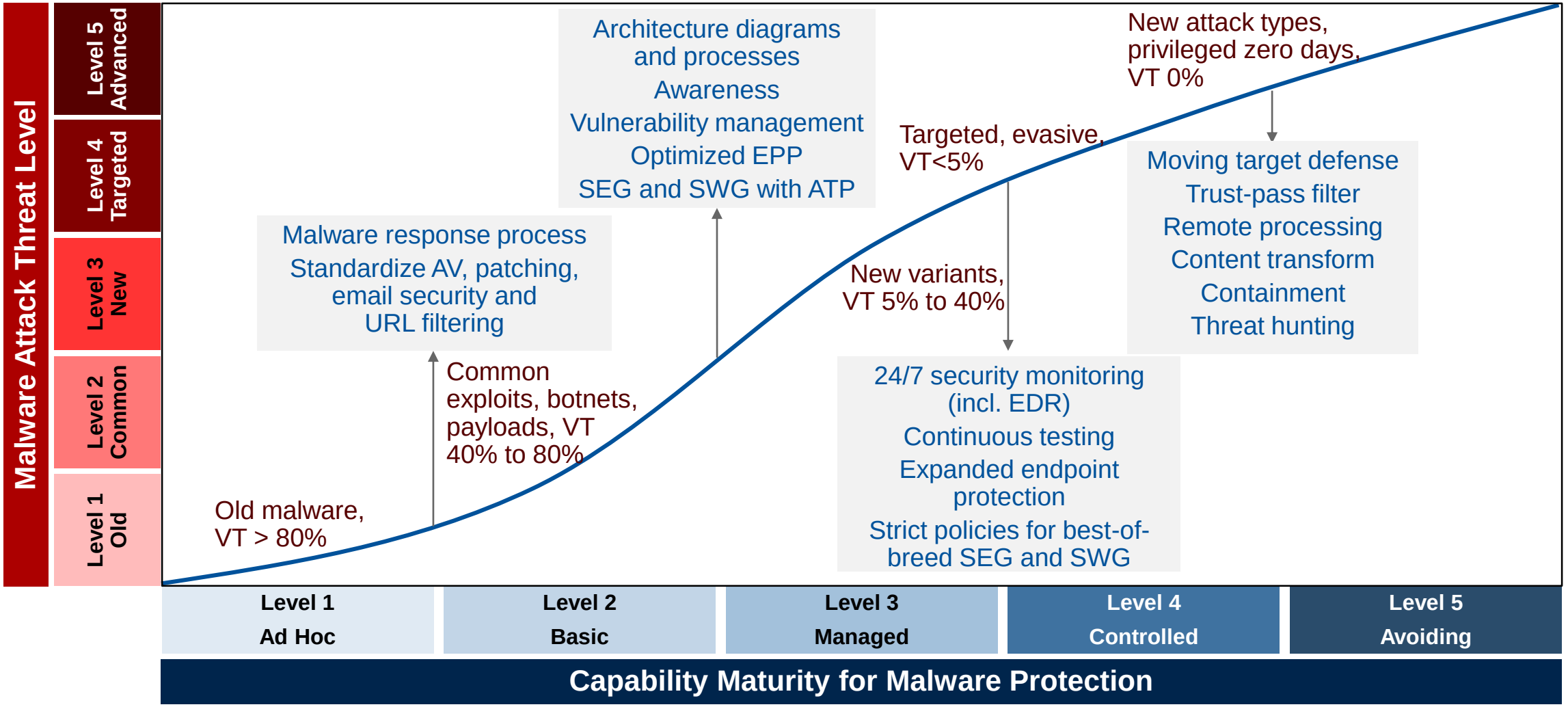
Gartner Security & Risk Management Summit
Summit 2018
04 – 07 June 2018 / National Harbor, MD

Tutorial: How to Architect Malware Protection

Mario de Boer


What secure web gateway features protect against malware?
How do I improve my endpoint protection?
How do I enhance my email gateway to protect my users against ransomware?
Mount web
Mount endpoint
Mount email

Malware Protection Maturity Must Match Attack Levels



VT: VirusTotal

Gartner

Level 1

Threat Level 1: Old Techniques

Infection techniques

- Email attachment containing old, executable, payload or droppers
- Old malware files on USB
- Direct download of old malware payload from internet (e.g., weaponized freeware)

Payload techniques

- Widespread malware payloads (executables, scripts) with hashes known for at least months
- Using common command and control (C&C) channels with known malicious IP addresses
- VT detection above 80% (all but the weakest solutions would catch it)

Old malware, still floating around on USB, backups and email inboxes

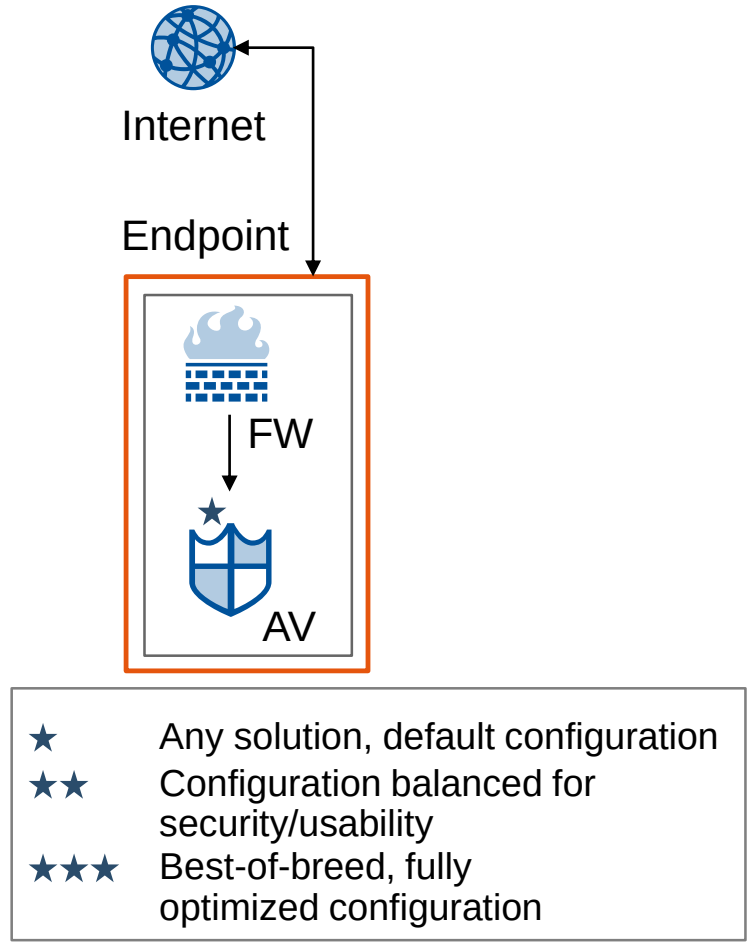
Gartner

Maturity Level 1: Initial

- **Process:**
  - Undefined, ad hoc, unrepeatable outcomes.
  - Heavy reliance on individuals "doing the right thing."
  - Outbreaks require huge mitigation effort, if discovered.
- **Controls:**
  - Inconsistent use of technology.
  - Lack of centrally enforced network and endpoint controls.
  - Major dependency on OS vendors and user configurations.

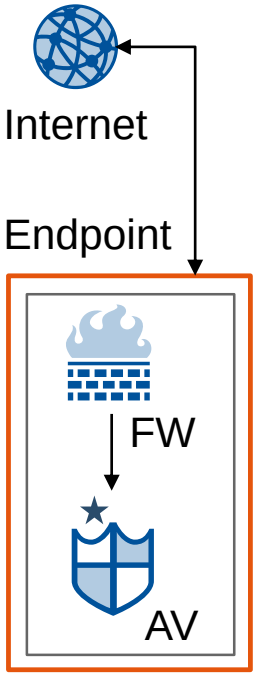
! Lack processes and standardization

No centralized email and web security



Gartner

Attacker's View on Maturity Level 1: Initial



- ★ Any solution, default configuration
- ★★ Configuration balanced for security/usability
- ★★★ Best-of-breed, fully optimized configuration

- Have users **download and install** malware (social engineering)
- Exploit **missing patches** through web, email or network
- **Reuse** existing malware, not too old
- Drop new payloads on endpoints that are **already compromised**
- **… too many trivial ways to compromise endpoints at very low cost**

Level 2

Threat Level 2: Common Techniques

Infection techniques

- Exploit of a known, and old, vulnerability (with patch at least 3 months old) in a client application commonly used for processing tainted content (browser, PDF reader, Microsoft Office)

Payload techniques

- Trivial variants of common malware (e.g., adding a character)
- Variations in used IP addresses, file hashes, but reuse of major components, behavior and infection methods
- VT detection between 40% to 80% (i.e., most solutions would catch it)

Infection through fully opportunistic, ad hoc and commonly available means (no customization)

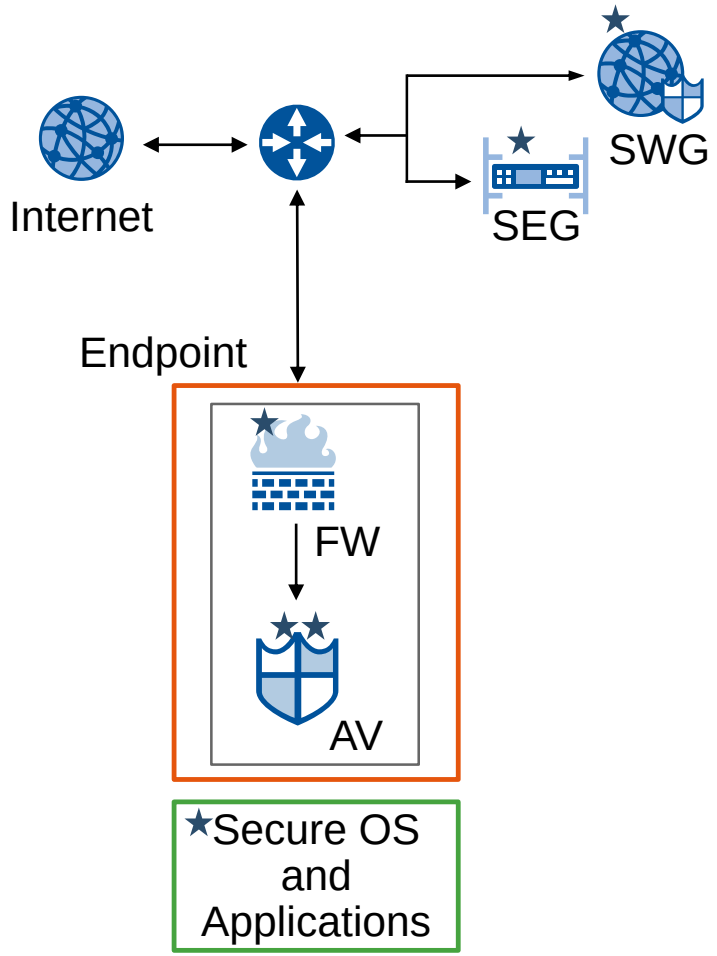
Gartner

Maturity Level 2: Reactive/Basic

- **Process:**
  - Malware response processes are not holistic, but rather apply to endpoints, email and web in silos.
  - Endpoint antivirus and OS patch management is somewhat centralized, typically in the desktop management group.
- **Controls:**
  - Centrally managed antivirus and OS patching.
  - Email security solution and URL filtering.
  - Mobile devices require minimum versions.

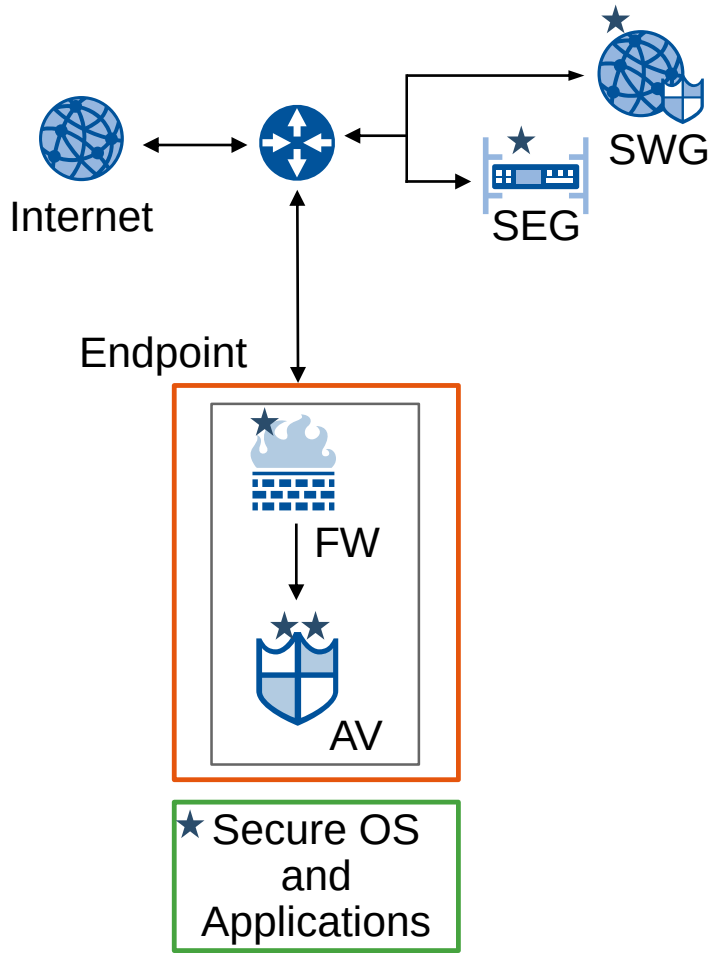
! Missing architecture diagrams and awareness training.

No vulnerability management. SEG and SWG are basic.



Gartner

Attacker's View on Maturity Level 2



- Use **new or benign URLs** for exploit or payload
- **Phish** user: Lure into opening attachment or click links
- Exploit **missing patches** in applications, typically through web or email
- Use **nontrivial variants** of malware (fail detection in low-end SEG, SWG and AV)
- **… Nothing that cannot be achieved by leveraging a good exploit kit and/or spam botnet**

Level 3

Threat Level 3: New Techniques

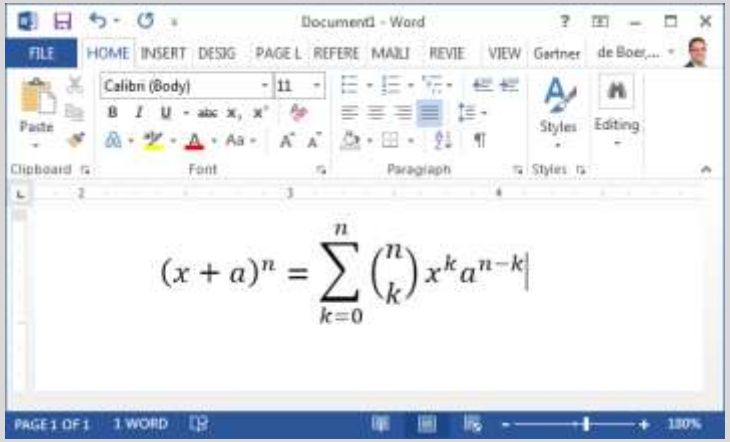
Infection techniques

- Exploit of a known, but recent, vulnerability (at most 3 months old) in a client application commonly used for processing tainted content (browser, PDF reader, Office)
- Fully automated lateral spread

Payload techniques

- Quickly morphing variants of common malware, but reuse of behavior
- Files obfuscated to evade detection by the majority of standard AV and poor sandboxes
- Standard fileless techniques
- VT detection 5% to 40% (i.e., strong solutions would likely catch it)

Use of polymorphism to reach maximum infection without becoming targeted



CVE-2018-0798, 0801, 0802, 0804-0807, 0812, 0845, 0848, 0849, 0862 (at time of writing)

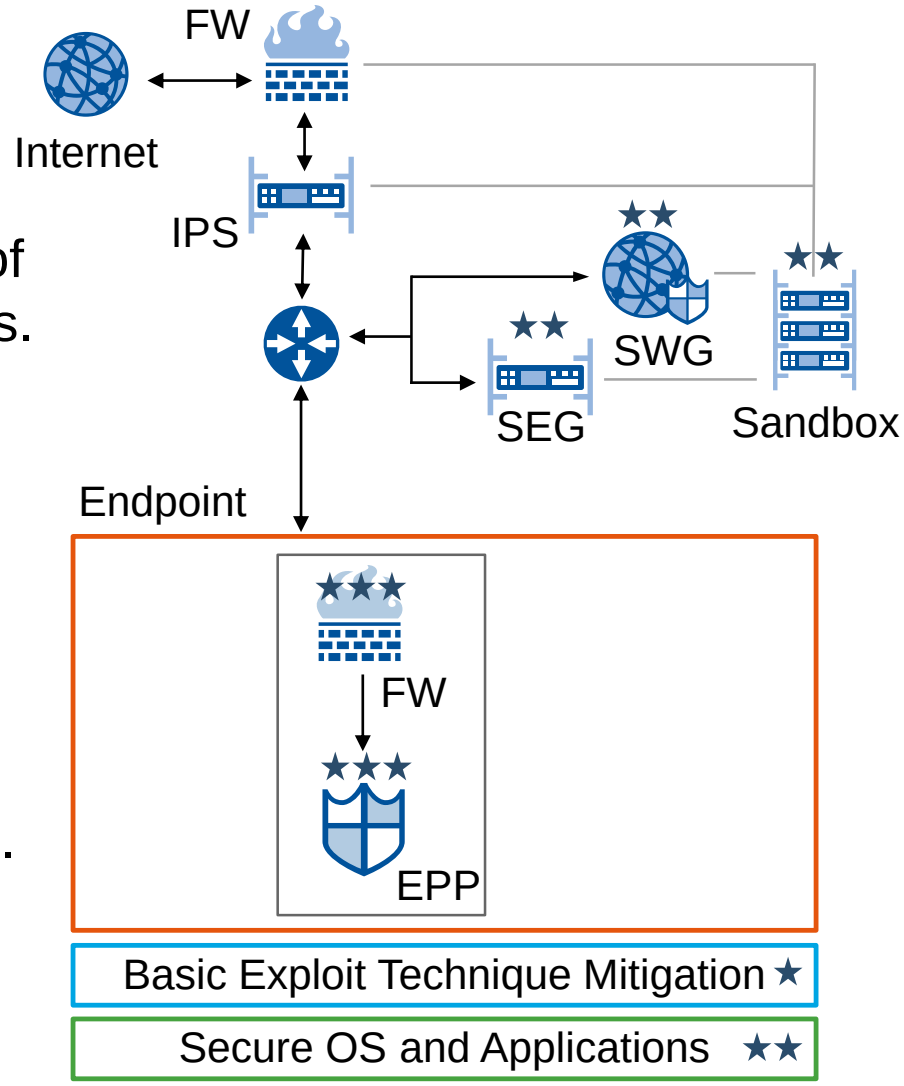
Gartner

Maturity Level 3: Managed

- **Process:**
  - Up-to-date architecture diagrams overreaching all aspects of malware protection across the network, endpoints and users.
  - Rigorous process descriptions for malware detection in security monitoring and anti-phishing awareness training.
- **Controls:**
  - Standardized endpoints, best-of-breed EPP, least privilege.
  - SEG: Spoof protection, authentication, tagging, multi-AV.
  - URL check and rewrite in SEG, sandbox for SEG and SWG.

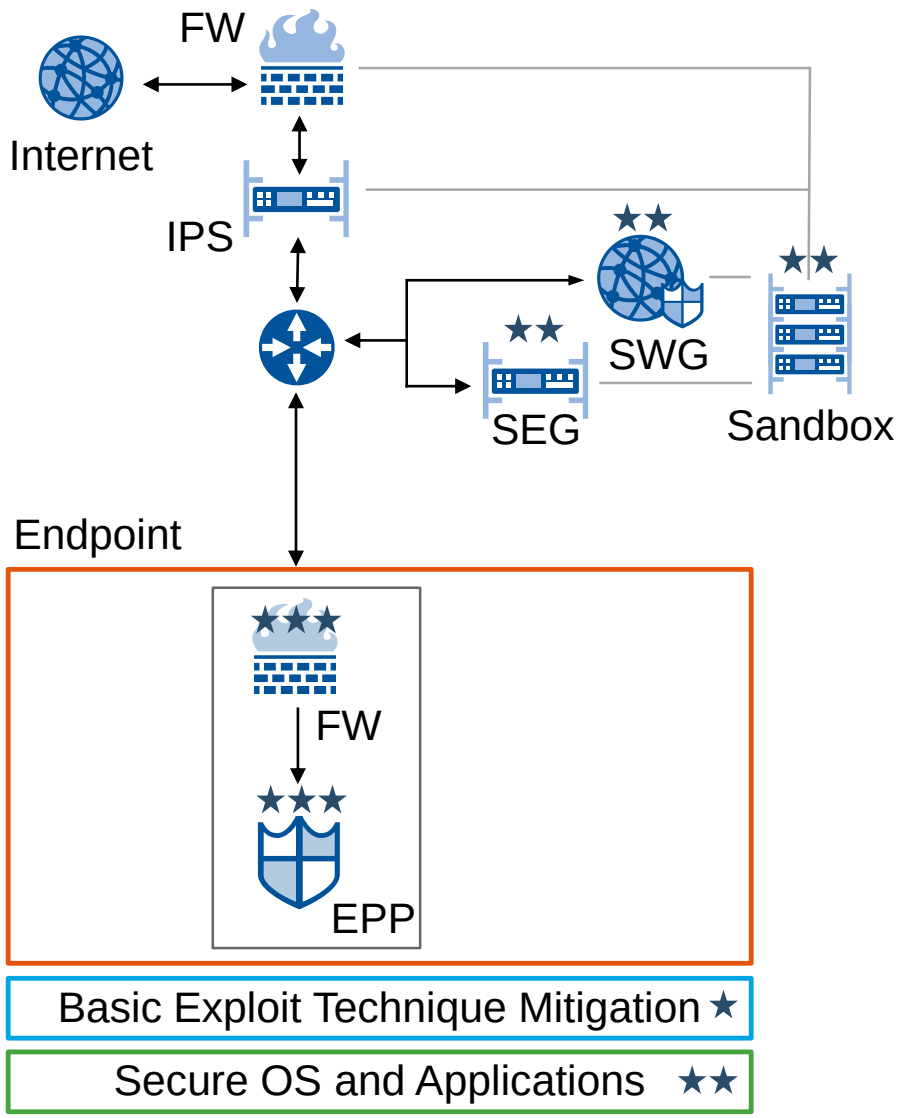
No 24/7 monitoring, lack of security awareness beyond email

Lack of EPP enhancements. SEG and SWG not best-of-breed



Gartner

Attacker's View on Maturity Level 3



- Use exploits to **very recent vulnerabilities:** Exploits must be advanced enough to evade basic mitigations such as DEP, ASLR, heap spray
- Use **sandbox evasion** techniques or use file types not covered by common sandboxes
- Sandbox may be set up to detect-only: Exploit the **process**
- Use evasive **fileless attacks** to infect, spread and for obtaining persistence
- **Evade rule-based** behavior analysis and signatures
- **… Achievable by leveraging strongest exploit kits, customization required**

Level 4

Threat Level 4: Targeted

Infection techniques

- Zero day in client application
- Crafty exploit, known technique, adapted for new applications or new OS
- Manual lateral spread (e.g., after server compromise)

Payload techniques

- Obfuscated to evade detection by leading sandboxes; no reuse of common attack identifiers; advanced fileless attacks
- Stealth to defeat detection (e.g., masquerading as benign, indicator removal from host and tools)
- VT detection < 5% (i.e., only the strongest have a small chance to detect)

Targeted attack, initiated by person, evading detection by solutions used by target

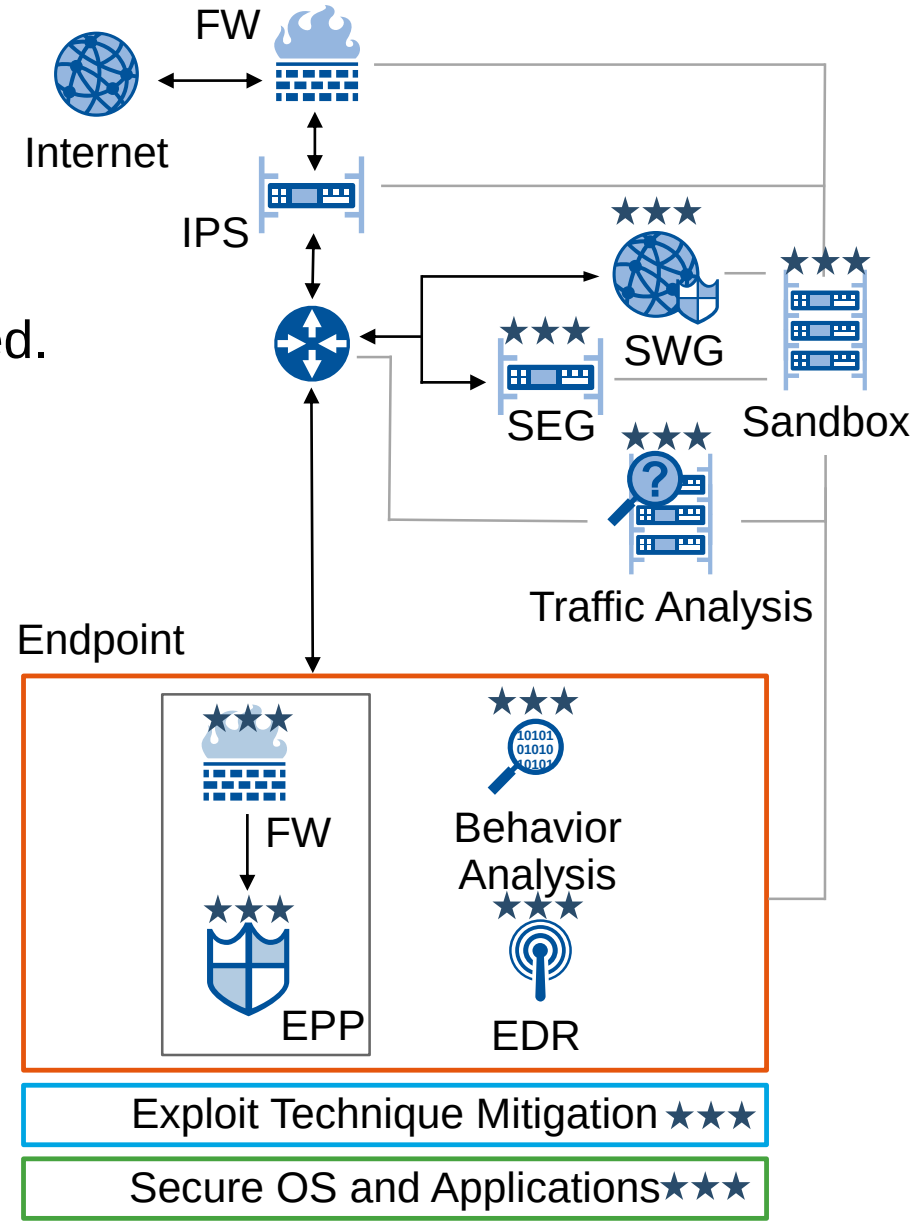
Gartner

Maturity Level 4: Controlled

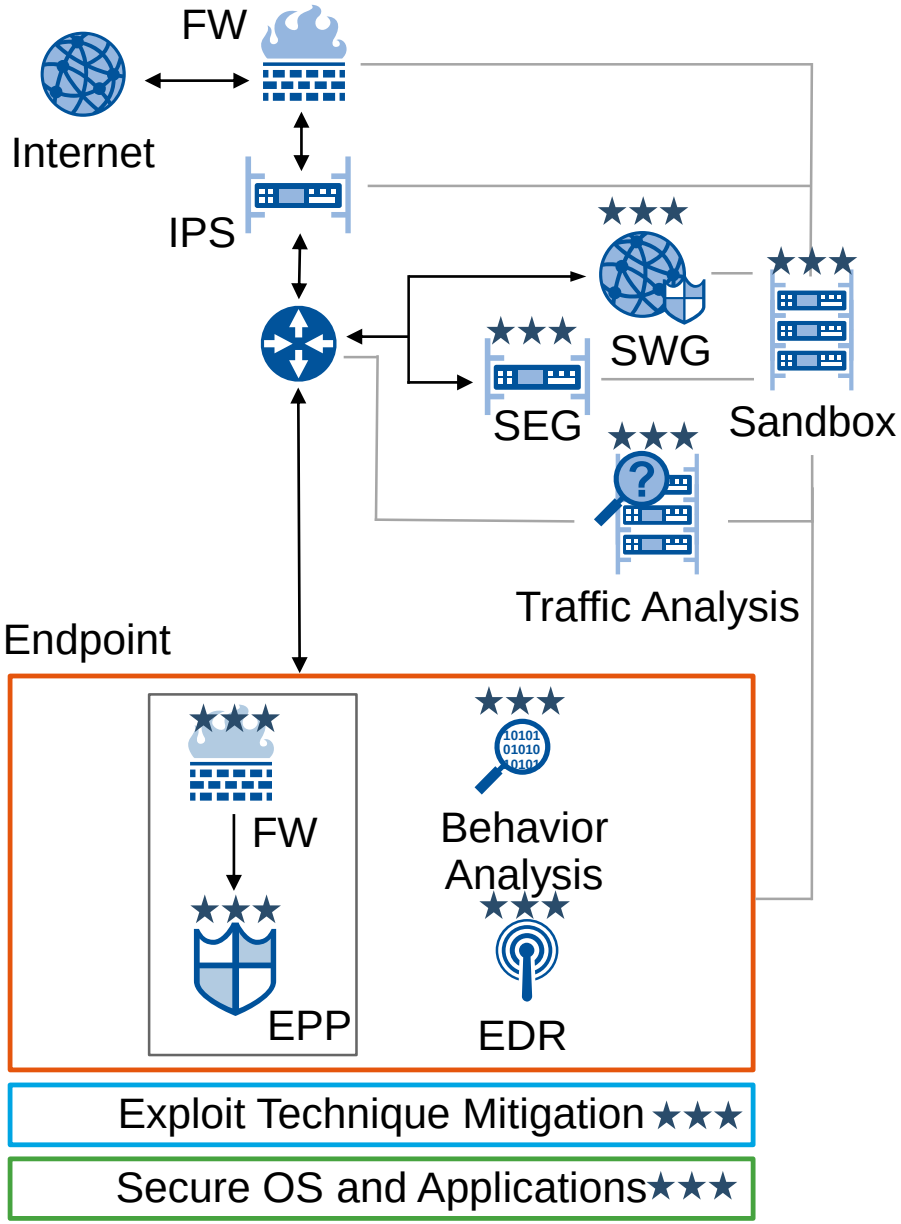
- **Process:**
  - Malware protection and response is predictable and controlled.
  - Quality and performance are understood and continuously tested across all malware protection processes.
  - Brand protection services and phishing awareness.
- **Controls:**
  - Best-of-breed solutions across all channels, fully optimized for prevention and detection. MTD across mobile devices.
  - In SaaS-heavy environments, CASB functionality.

! Security awareness not fully embedded, lack of hunting

Protection technologies are a part of assets under attack.



Attacker's View on Maturity Level 4



- Deep social engineering; **no reuse of asset** (IP, sender, malware component) of poor reputation
- **New exploit techniques** on zero days
- Use best-of-breed **evasion** across all static and dynamic analysis techniques used by target
- **Remove traces** of attacks and interfere with network and endpoint detection technologies
- **Hide** from any detection and prevention processes
- **… Requires manual effort by attacker, significant cost and effort**

Level 5

Threat Level 5: Advanced Techniques

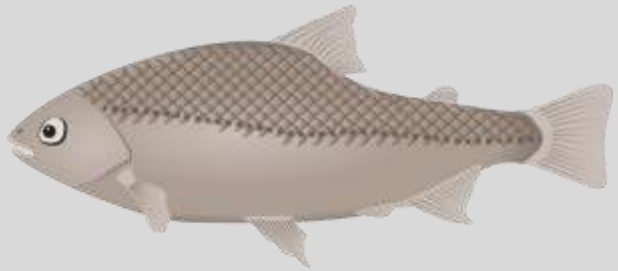
Infection techniques

- Zero-day exploit leveraging new techniques
- Exploit in privileged code
- Firmware/BIOS persistency
- Malware plant through physical access

Payload techniques

- Known benign, signed or in-memory only
- Hidden in firmware or other components not visible to OS
- Advanced evasion across multiple layers; not detectable by basic indicators
- No or greatly obfuscated communication
- VT detection 0% (i.e., no file AV will detect it)

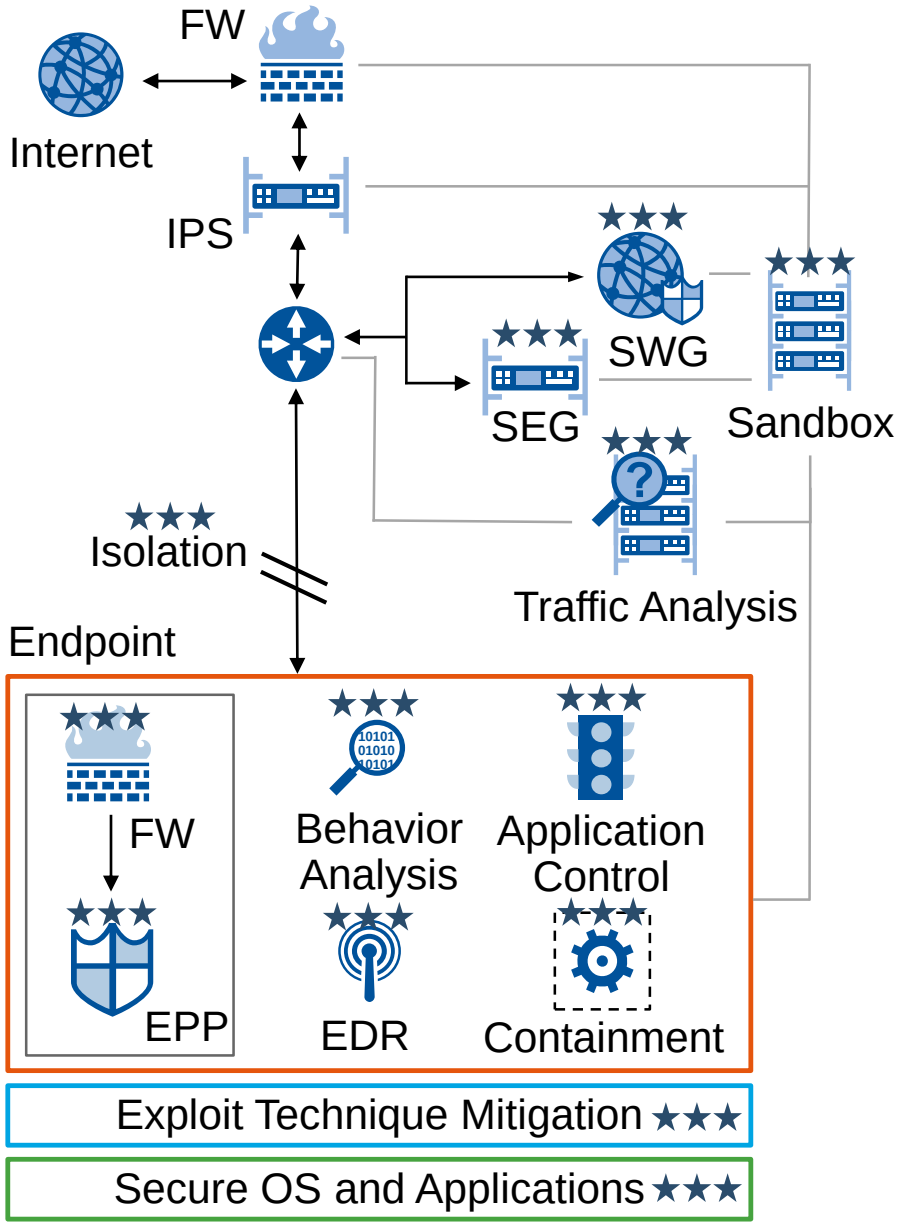
New attack type leveraging exploits in privileged code, with completely new payload types, highly evasive and targeted



Gartner

Maturity Level 5: Avoiding

- **Process:**
  - Innovative technologies and continuous optimization.
  - Change controls continuously.
  - Use advanced detection and threat hunting, and embed security awareness in all user workflows.
- **Controls:**
  - Moving target defense.
  - Trust-pass filter.
  - Remote processing/isolation.
  - Content transform.
  - Containment.



Recommendations

Gartner

Recommendations

- ✓ **Identify** the strengths, scope and imbalances **for the current malware protection capability** by using the Capability Maturity Model presented in this research.
  This results in an understanding of the level of malware attacks that you are protected against.
- ✓ **Define a future protection architecture** that matches the attack scenarios you need protection against by designing processes — as well as endpoint, email and web controls — that protect against attacks corresponding to the identified attack scenarios.
- ✓ **Communicate** your protection level goals and have the business accept residual risks.

Recommendations

- ✓ **Improve the maturity** of malware protection architecture across endpoints and the network **by defining a roadmap** while leveraging the five maturity levels defined in this assessment.
- ✓ **Improve** malware protection maturity **step by step.** With most malware attacks taking place at threat Levels 1 through 3, all organizations should have an ambition to reach at least maturity Level 3 — and many should strive for maturity Level 4.

Recommended Gartner Research

- **Improving Malware Protection Maturity by Using Attack Scenarios**
  Mario de Boer (G00317553)
- **Comparing Endpoint Technologies for Malware Protection**
  Mario de Boer (G00337398)
- **Beyond Detection: 5 Core Security Patterns to Prevent Highly Evasive Attacks**
  Mario de Boer (G00346997)
- **How to Plan, Implement and Operate a Successful Application Whitelisting Deployment**
  Jon Amato (G00343685)

For information, please contact your Gartner representative.

Gartner

Appendix: Maturity Model Details

Malware Protection Maturity Model Across Architecture

Level	Indicators
Level 1: Ad Hoc	Missing processes (no or purely ad hoc policy management, reporting and response) No integration between solutions No security awareness activities
Level 2: Basic	Documented response processes fully reliant on existing endpoint, email and web malware protection solutions, in isolation Processes for managing AV, email security and URL filtering disconnected
Level 3: Managed	Up-to-date detailed architecture diagrams for all components involved in malware protection SIEM with SWG, SEG, firewall (FW) and intrusion prevention system (IPS) log sources used for monitoring and malware incident response Anti-phishing awareness training
Level 4: Controlled	Exchange, and use of threat intelligence between malware protection solutions Quantitative indicators used throughout malware protection processes Fully operational 24/7 security monitoring based on endpoint OS events, EDR, EPP, SEG, SWG and network (FW, IPS and network traffic analysis [NTA]) events SLA with third party for malware response (investigation and remediation) Brand protection services (tracking domain registrations, brand abuse, social media, etc.) Continuous testing of malware detection, prevention and remediation capabilities Security awareness training beyond anti-phishing
Level 5: Avoiding	Continuously improving, adapting architecture for malware, fully integrated across client and server endpoints and network Internal malware reverse engineering capabilities Threat hunting across endpoints and the network Security awareness embedded in all end-user workflows

Gartner

Capability Maturity Model for Endpoint Malware Protection

Level	Indicators
Level 1: Ad Hoc	▪ Some AV (often different solutions in an organization) with unknown, or default, configuration ▪ No centralized management or reporting ▪ Local admin in use by regular users ▪ No coordinated patching
Level 2: Basic	▪ Managed AV (mainly signatures and heuristics) across client and server endpoints ▪ Local admin allowed by exception (groups of users) ▪ Coordinated OS patching ▪ Endpoint backups ▪ Require minimum versions (without known critical vulnerabilities) for mobile devices
Level 3: Managed	▪ Centrally managed EPP with audited optimized setting (i.e., optimized for detection): use of a combination of basic memory protection and exploit mitigation (data execution prevention [DEP], address space layout randomization [ASLR] and heap spray) on all endpoints ▪ Standardized hardware and golden images for client endpoints ▪ Least-privilege management ▪ Control of removable media ▪ Centralized management and reporting on vulnerabilities and patches with clear SLA ▪ Use EMM to manage mobile devices
Level 4: Controlled	▪ EPP with extensive support for modern detection methods such as machine learning ▪ Best-of-breed behavior analysis to detect and block malware and nonmalware attacks on all endpoints ▪ Extensive memory protection capabilities (beyond DEP, ASLR and heap spray mitigations) ▪ Selective use of application whitelisting (for static client endpoints and some server roles) and EDR for specific categories of endpoints ▪ Active management and monitoring of EPP and EDR events ▪ Mobile threat defense ▪ Attestation of unknown files before execution — for example, in a network sandbox ▪ Comprehensive server security suite across all physical, virtual servers and infrastructure as a service (IaaS) instances, including malware, host intrusion prevention system (HIPS), file integrity monitoring (FIM), virtual patching, application control and microsegmentation
Level 5: Avoiding	▪ Isolation of risky exposed processes across servers and client endpoints, though containment on the endpoint or browser isolation in network ▪ Use of hardware-supported technologies where available (control flow integrity [CFI] for memory protection, Intel Virtualization Technology for Directed Input/Output (VT-d) for containment and application control, trusted platform module [TPM] for integrity, etc.) ▪ Default-deny whitelisting (or data-level whitelisting), EDR and deception across all endpoints ▪ Advanced monitoring of all endpoint events and user and entity behaviors ▪ Endpoint forensics tools and practices

Capability Maturity Model for Email Malware Protection

Level	Indicators
Level 1: Ad Hoc	▪ No central AV for email, rely on endpoint and email provider (i.e., relying on ISP or cloud email service without good oversight)
Level 2: Basic	▪ Email gateway or email server with standard AV scanning of attachments, typically using a single AV engine ▪ Detection mainly based on reputation (e.g., spam blacklists and malware signatures) ▪ Block of executables in email attachments
Level 3: Managed	▪ Multilayer email protection (SEG, email inbox server and endpoint) ▪ Multi-AV scanning in SEG ▪ Email server hardening and monitoring ▪ Network sandbox integration (e.g., cloud-based) with SEG ▪ URL inspection on delivery (malware, phishing) and/or URL disarm and/or URL rewrite (redirection) ▪ Basic spoofing protection (e.g., email address mismatch) ▪ Sender Policy Framework (SPF) and/or DomainKeys Identified Mail (DKIM): inbound validation used in SEG, enforced for outbound ▪ Inbound email tagging
Level 4: Controlled	▪ Attachment control in the form of whitelisting file types ▪ Spoofing and impersonation detection ▪ Cousin domain detection ▪ Anomaly detection for business email compromise (BEC) and other low-prevalent attacks ("outlier detection") ▪ SPF, DKIM and Domain-Based Message Authentication, Reporting and Conformance (DMARC) for own domain and enforced for inbound ▪ Fully customizable advanced threat defense (ATD)/sandbox solution (on-premises) ▪ Integration with web for C&C correlation and reuse of categories ▪ Inbox access control (two-factor authentication (2FA), conditional access) ▪ Use of DLP for exfiltration detection
Level 5: Avoiding	▪ Content disarm and reconstruction on email attachments ▪ Strict attachment control: file type whitelisting per recipient/sender ▪ Remote viewing or local isolation of attachments ▪ Anomaly detection for internal email ▪ Digital signatures on all internal email and select external email

Capability Maturity Model for Web Malware Protection

Level	Indicators
Level 1: Ad Hoc	▪ No malware scan in web channels ▪ No, or inconsistent, URL filtering
Level 2: Basic	▪ URL filtering with policy to prevent visiting known malicious sites in SWG, firewall, router, IPS or endpoint
Level 3: Managed	▪ Centralized management and reporting for SWG spanning the organization. ▪ SWG with AV scanning and extensive protection against malicious websites not categorized as malicious (dynamic URL classification, real-time content inspection) ▪ Known exploit detection and prevention (vulnerability shielding) ▪ SWG for off-premises endpoints (either through endpoint, backhaul, or cloud SWG) ▪ Web application control (granular control of web applications beyond browsers) ▪ Network sandbox integration with SWG ▪ C&C detection ▪ SSL decryption
Level 4: Controlled	▪ Download control in the form of whitelisting file types ▪ Exploit detection and prevention for browsers and browser extensions capable of detecting new exploits ▪ Granular control over non-HTML content: whitelisting of Java, Flash and other content on a per user, per site basis ▪ Fully customizable sandbox solution (on-premises) ▪ Advanced threat detection covering behavior-based detection, anomalous traffic detection (egress) and exfiltration detection ▪ Integration with email for C&C correlation ▪ Use of DLP for exfiltration detection ▪ CASB functionality to detect and protect against malware in SaaS-heavy environments
Level 5: Avoiding	▪ CDR for downloaded content ▪ Full web browser isolation (remote browsing, local containment or network isolation) ▪ Strict download control: file type whitelisting per downloader and site

