Integrovaný DDI/NAC nástroj – nezbytnost při budování kybernetické ochrany organizace

AddNet

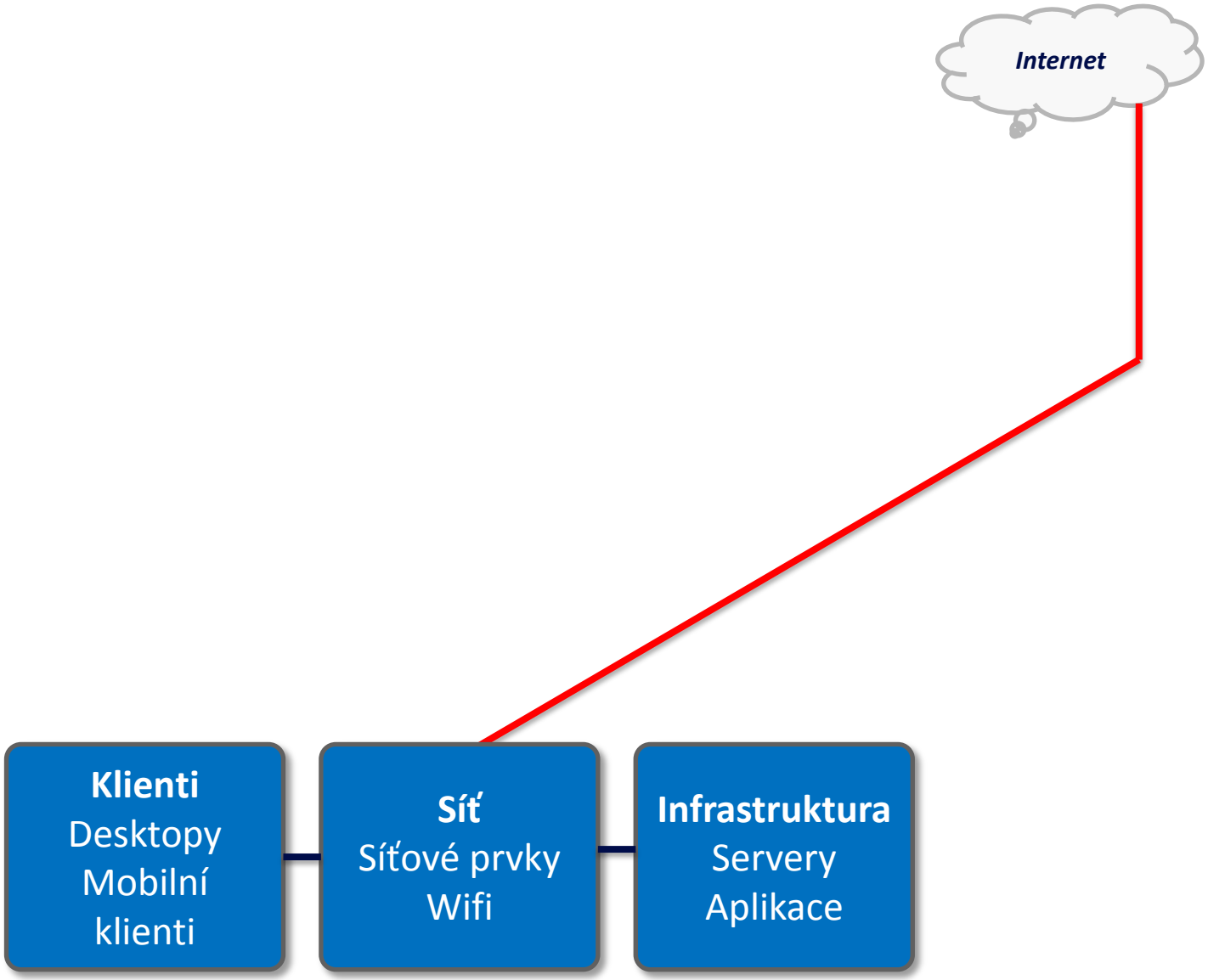
Jindřich Šavel

5.4.2016

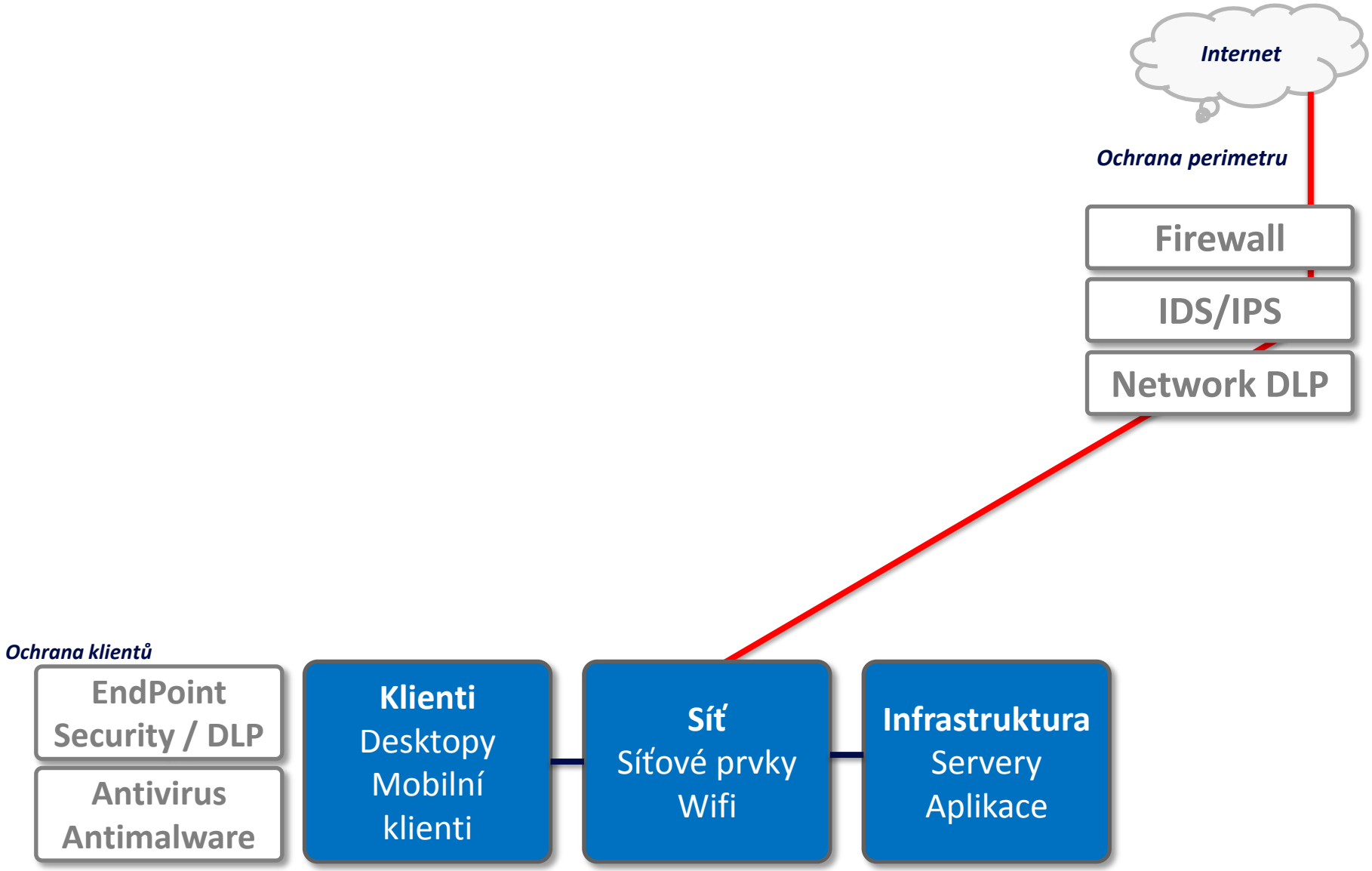
Koncept Aktivní bezpečnosti sítě

Koncept Aktivní bezpečnosti sítě

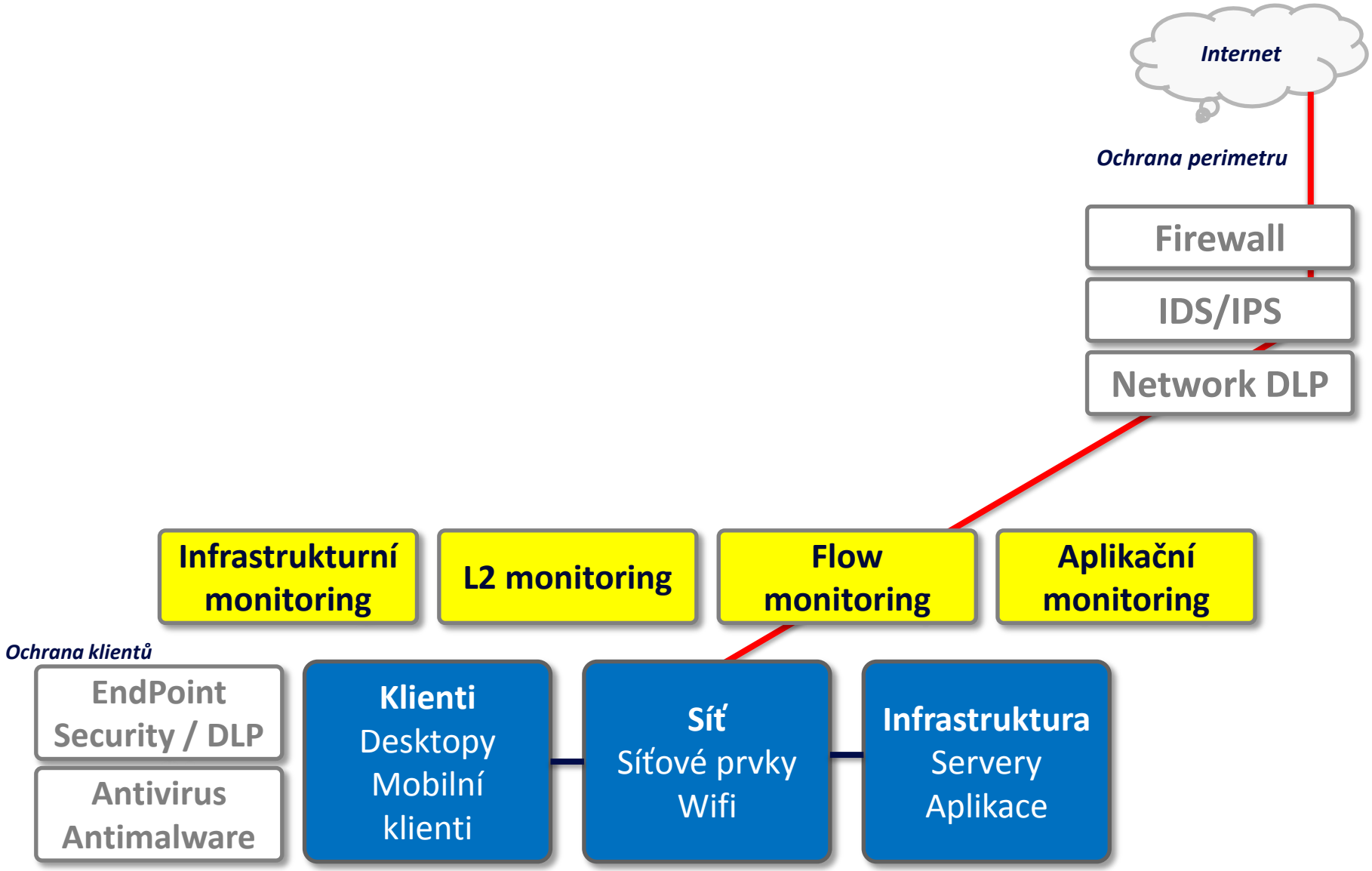
Koncept Aktivní bezpečnosti sítě



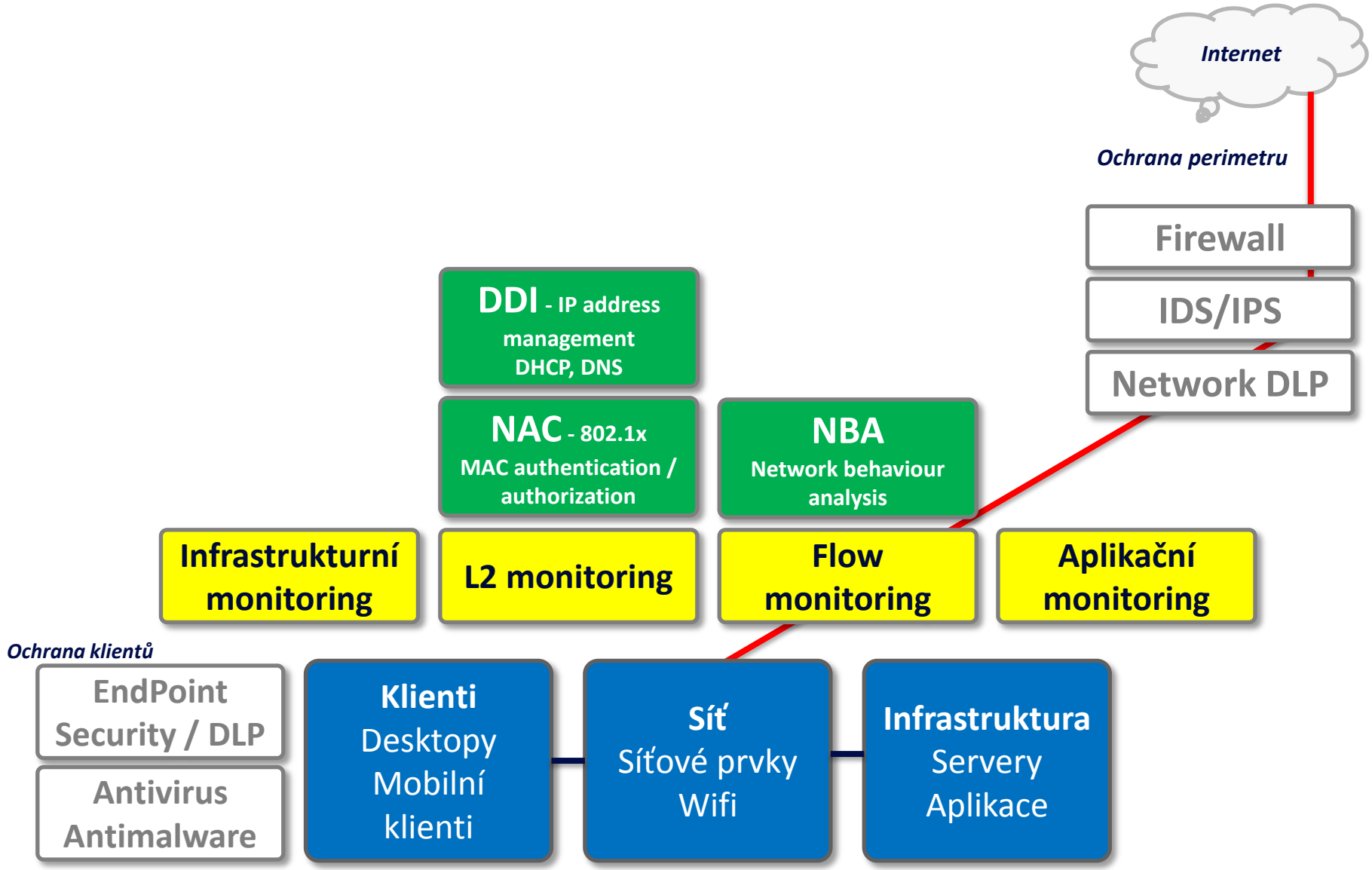
Koncept Aktivní bezpečnosti sítě



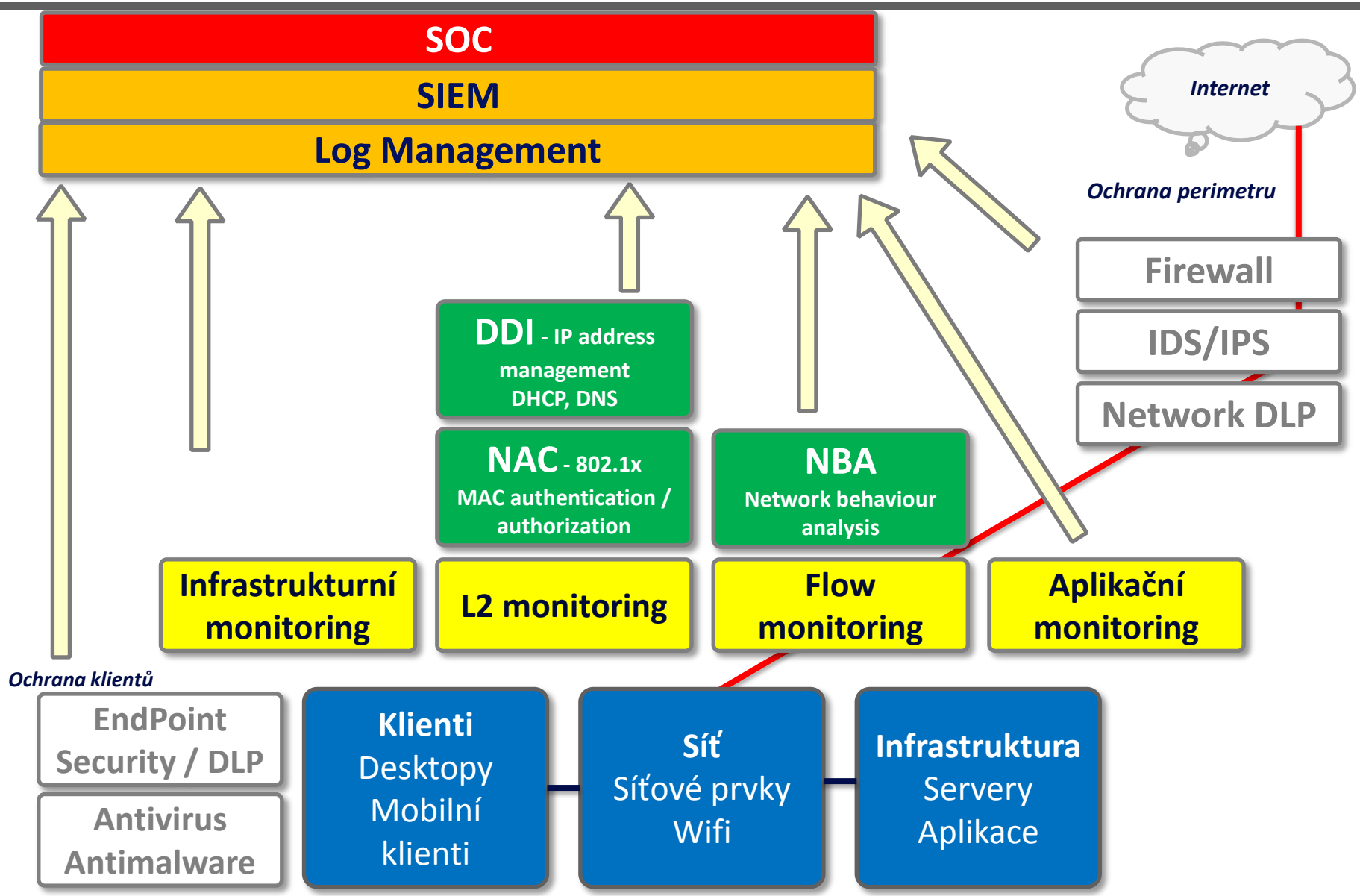
Koncept Aktivní bezpečnosti sítě



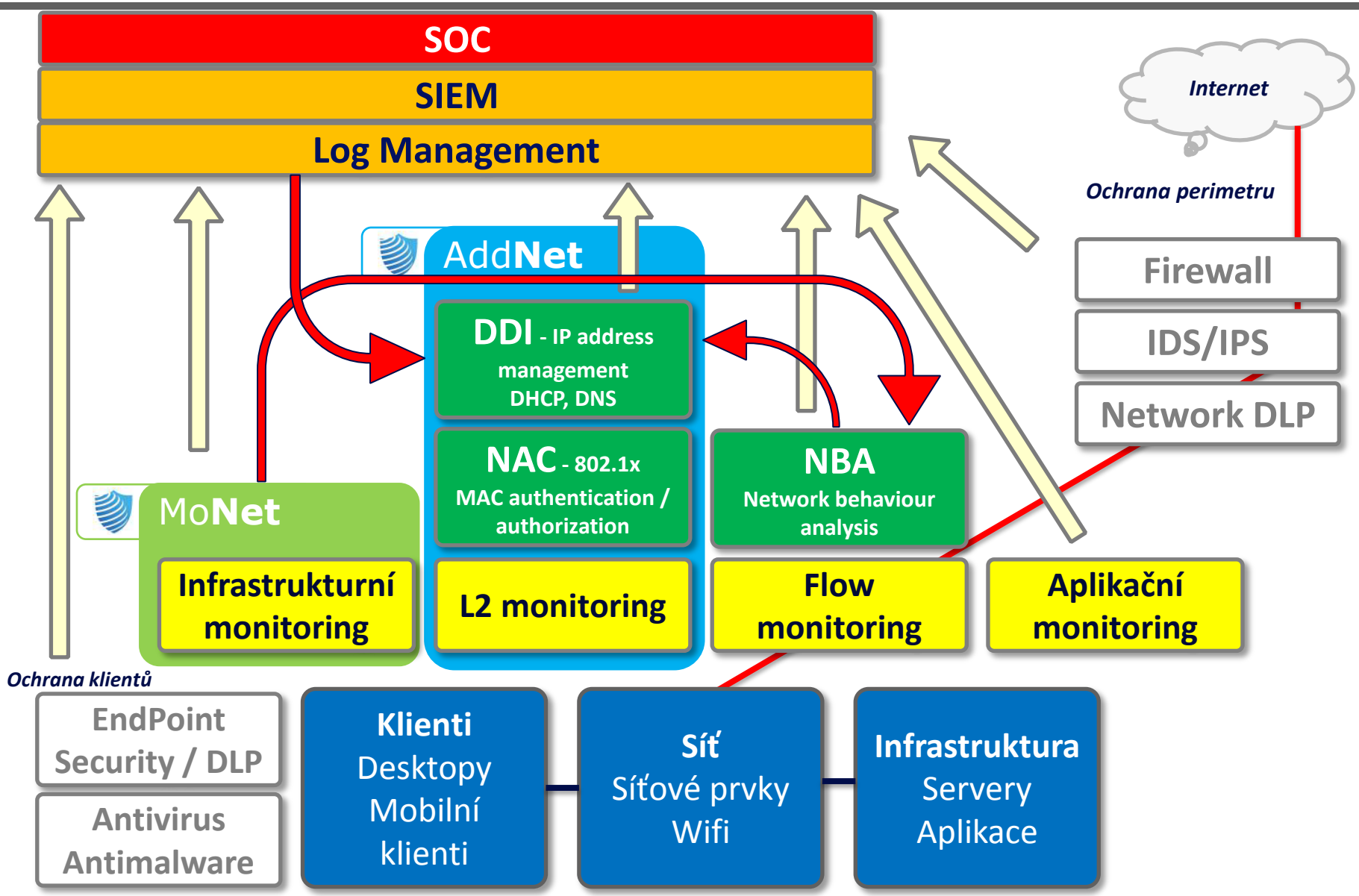
Koncept Aktivní bezpečnosti sítě



Koncept Aktivní bezpečnosti sítě



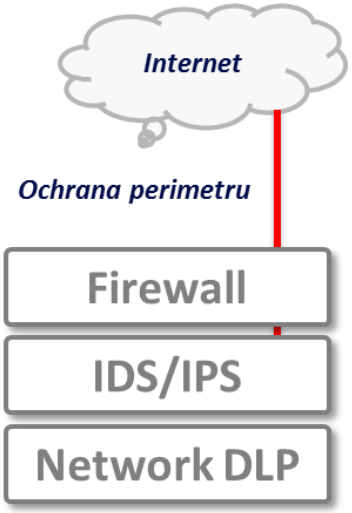
Koncept Aktivní bezpečnosti sítě



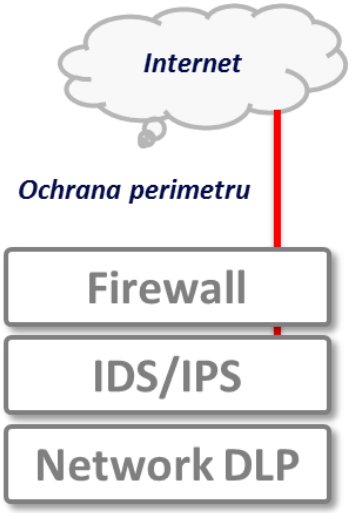
Bezpečnost vnitřní sítě

Bezpečnost vnitřní sítě

Bezpečnost vnitřní sítě



Bezpečnost vnitřní sítě

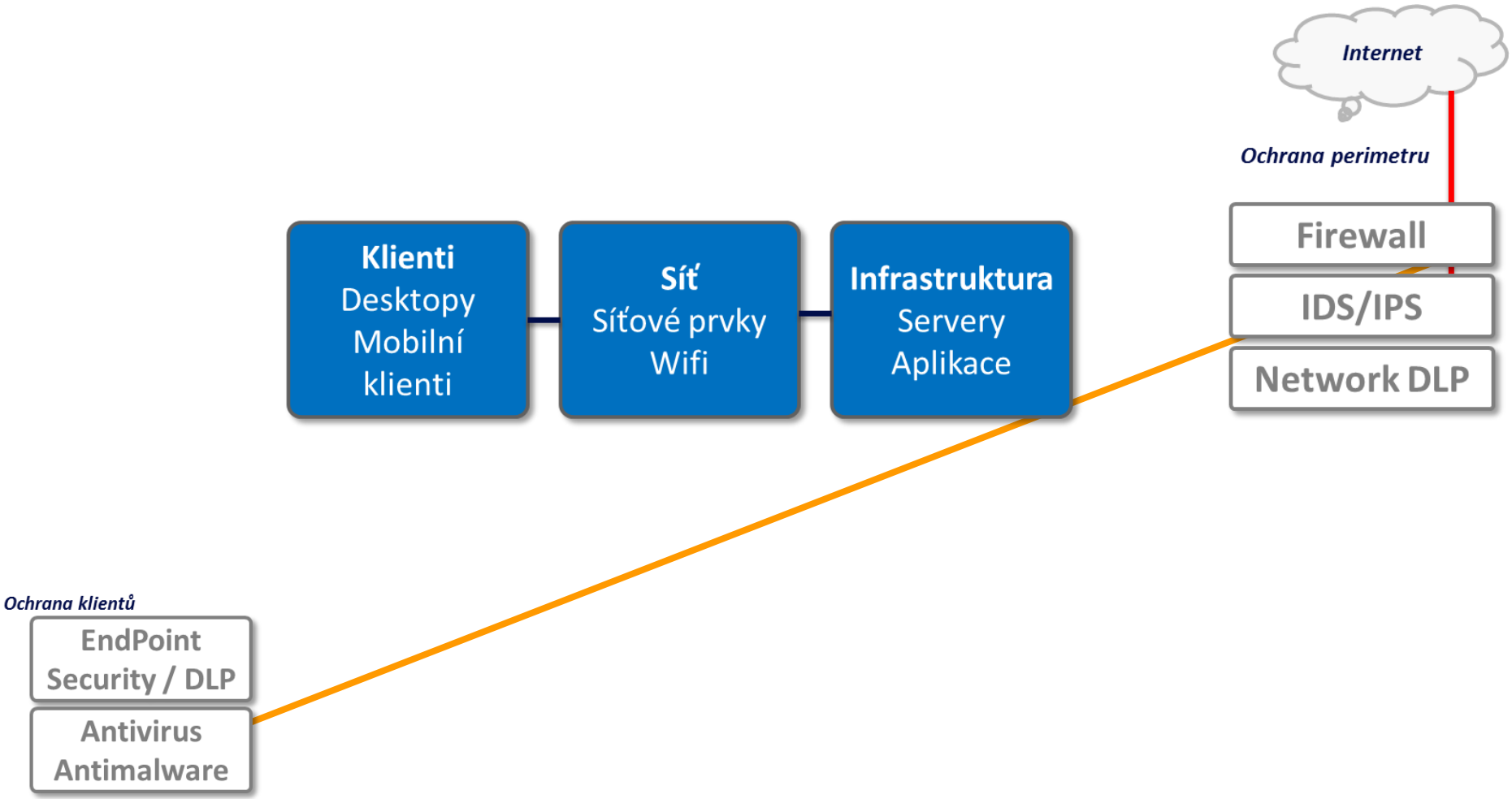


Ochrana klientů

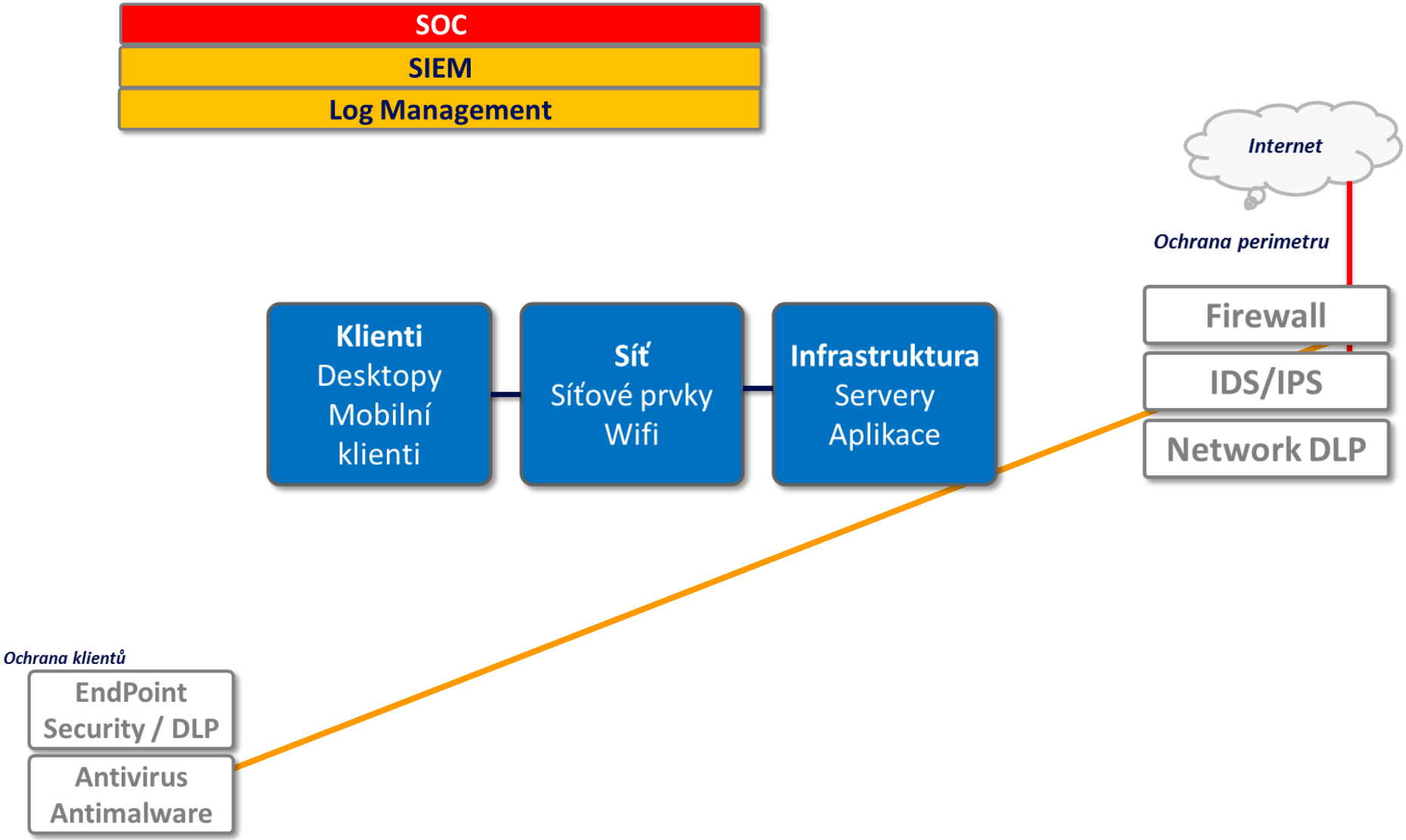
EndPoint Security / DLP

Antivirus Antimalware

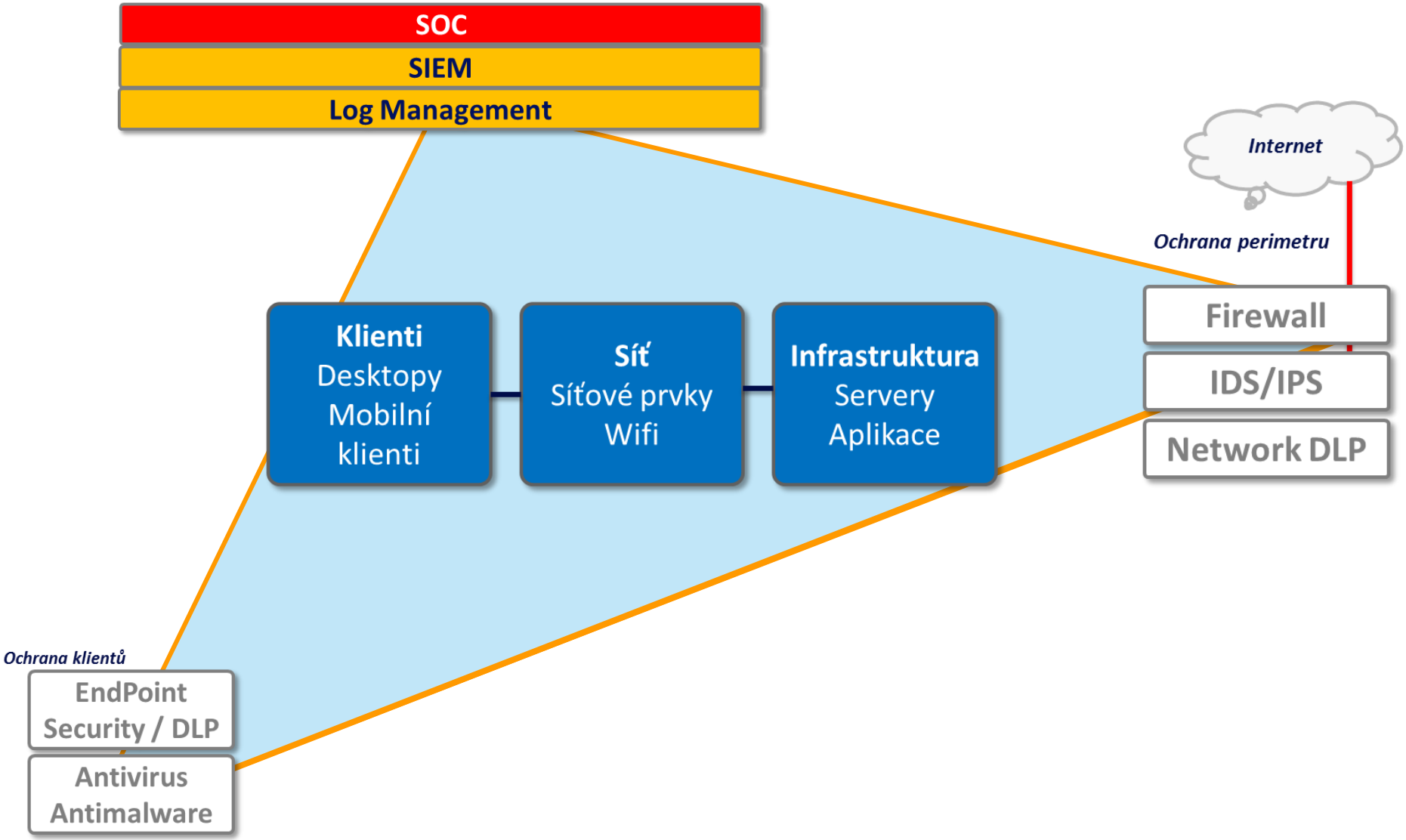
Bezpečnost vnitřní sítě



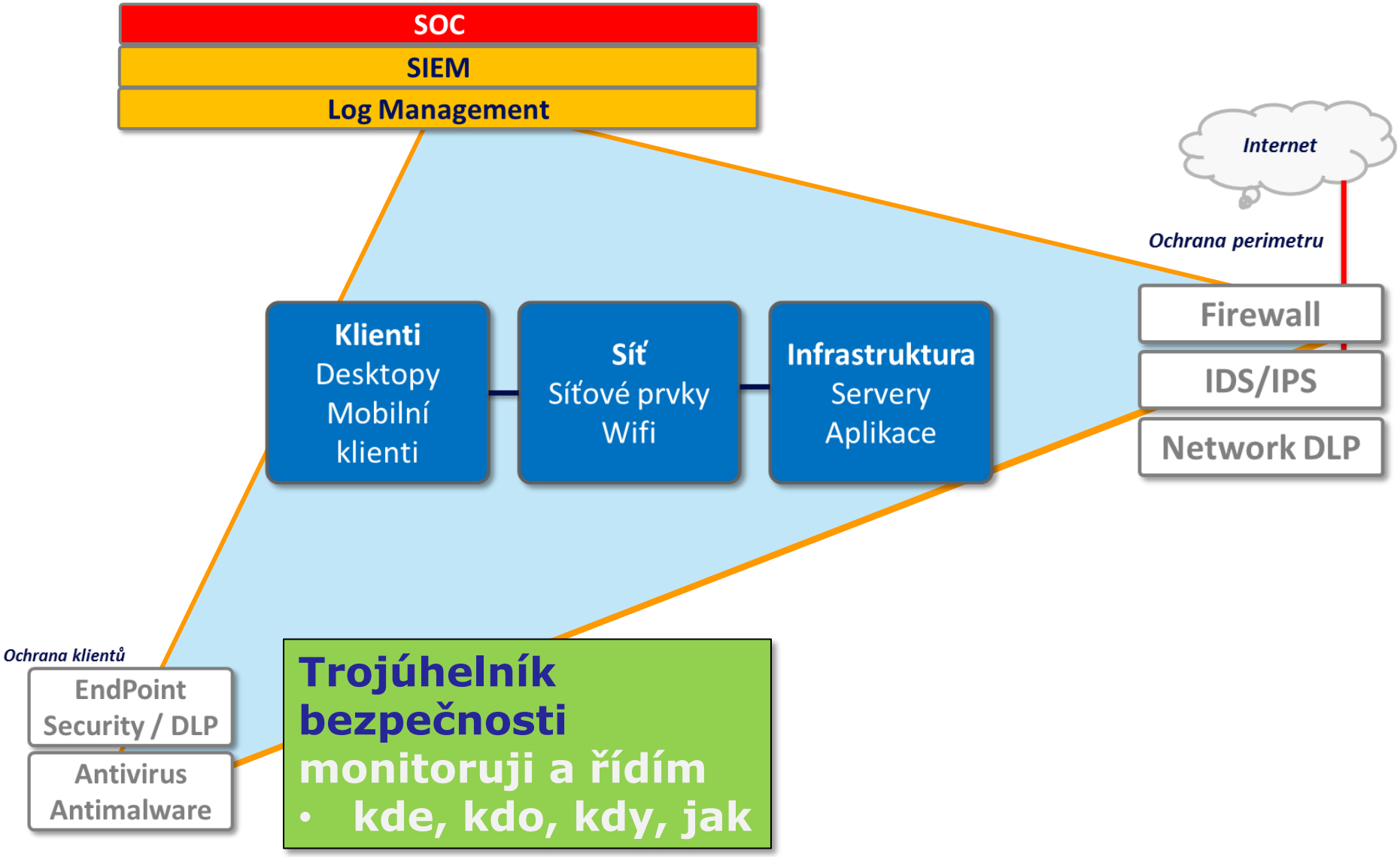
Bezpečnost vnitřní sítě



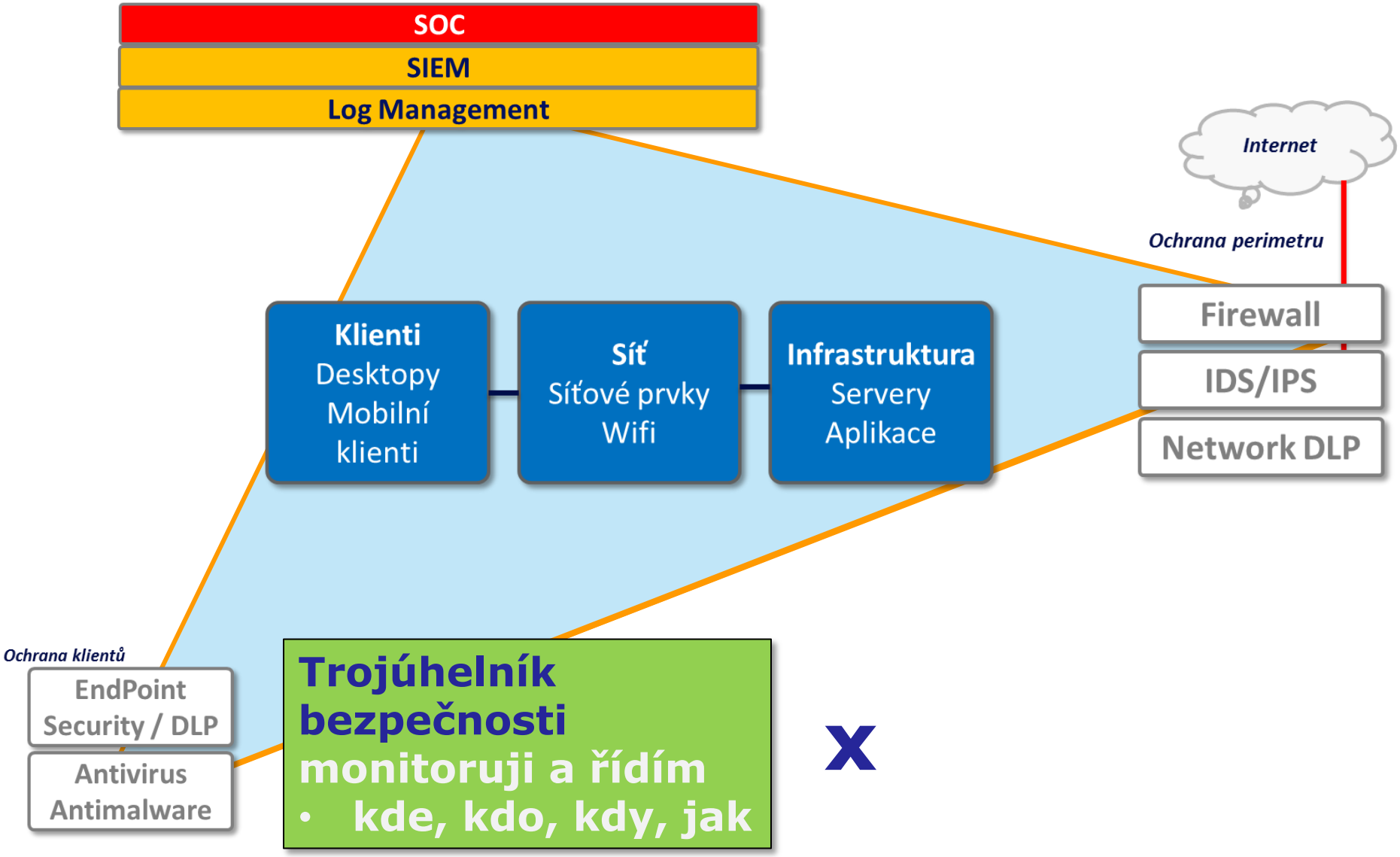
Bezpečnost vnitřní sítě



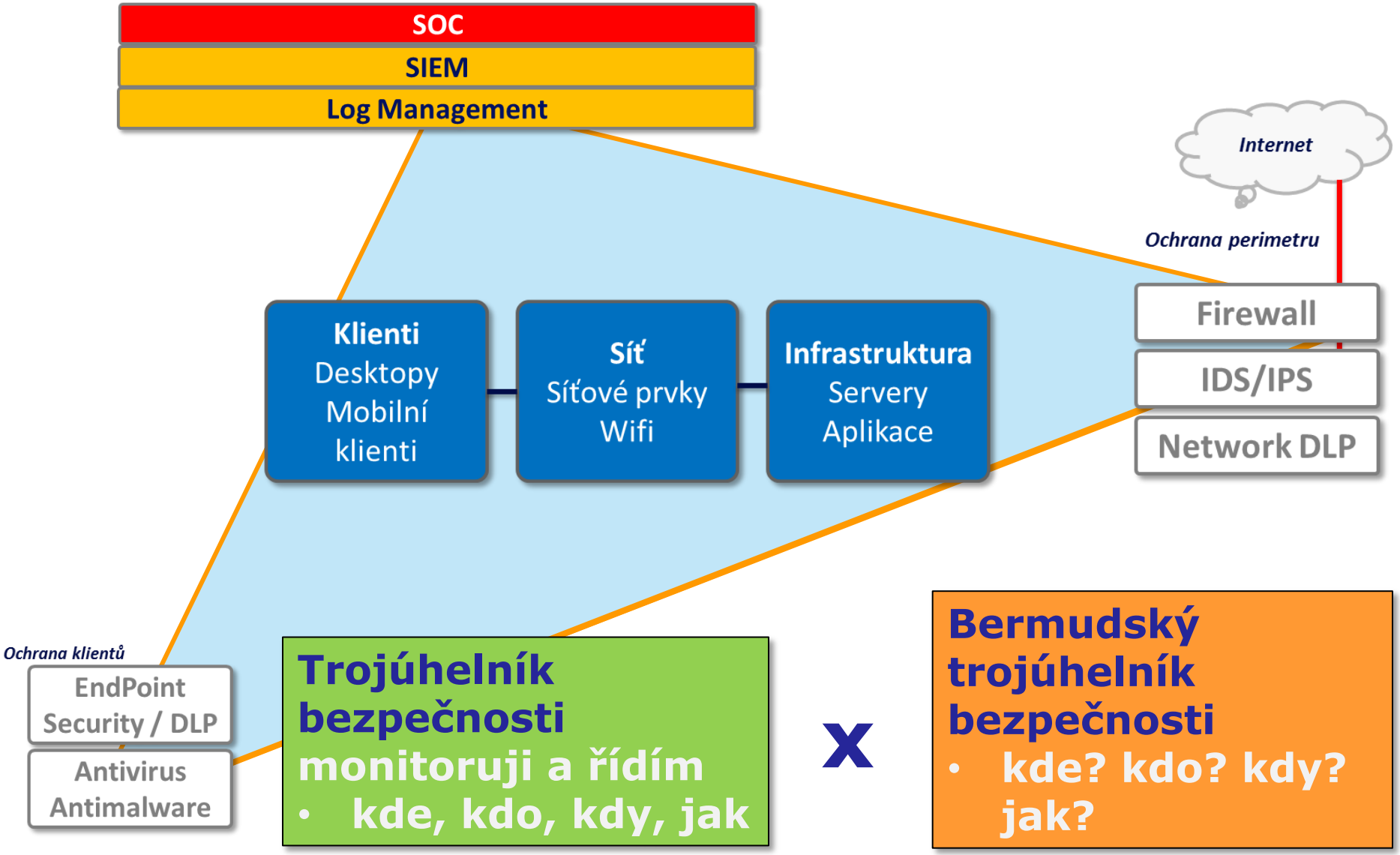
Bezpečnost vnitřní sítě



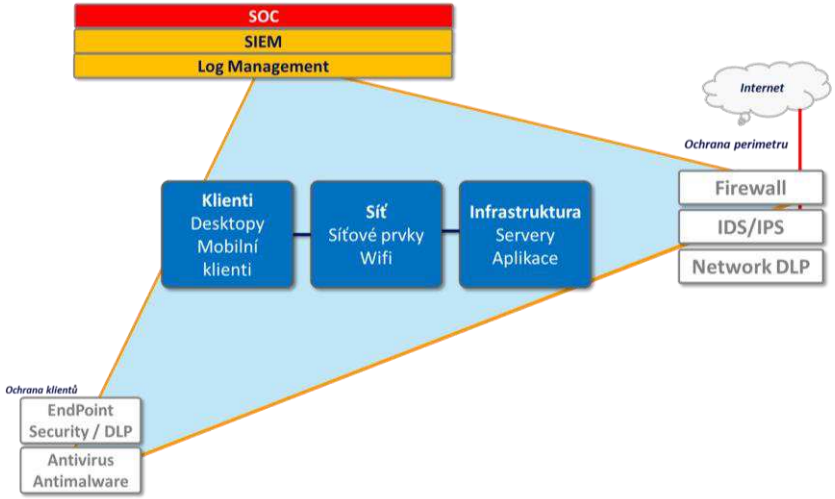
Bezpečnost vnitřní sítě



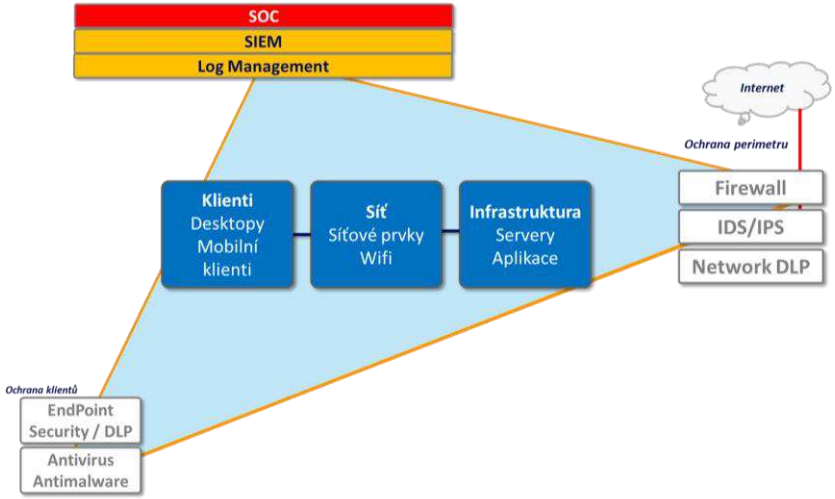
Bezpečnost vnitřní sítě



Bermudský trojúhelník bezpečnosti



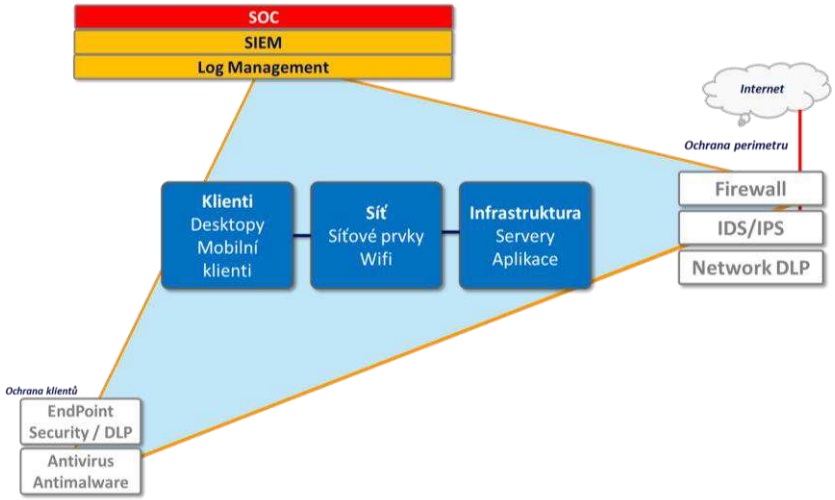
Bermudský trojúhelník bezpečnosti



Bermudský trojúhelník bezpečnosti

- **kde? kdo? kdy? jak?**

Bermudský trojúhelník bezpečnosti

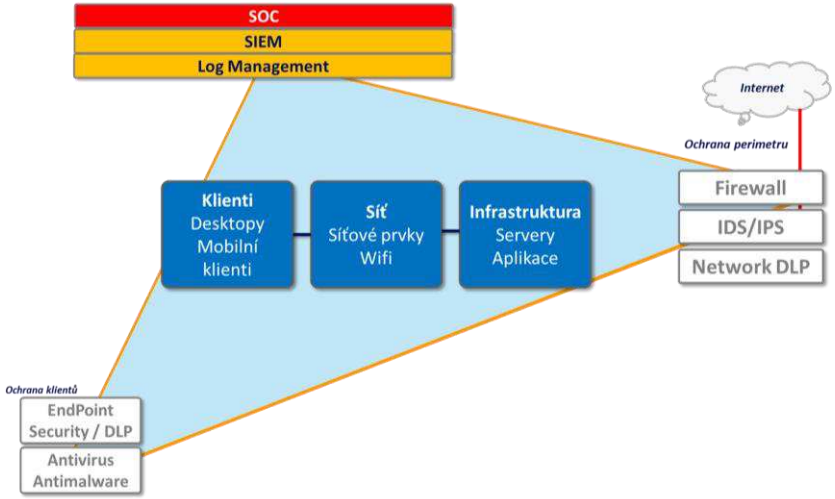


Bermudský trojúhelník bezpečnosti

- **kde? kdo? kdy? jak?**

- **Žádné řízení přístupu do sítě (NAC)**

Bermudský trojúhelník bezpečnosti

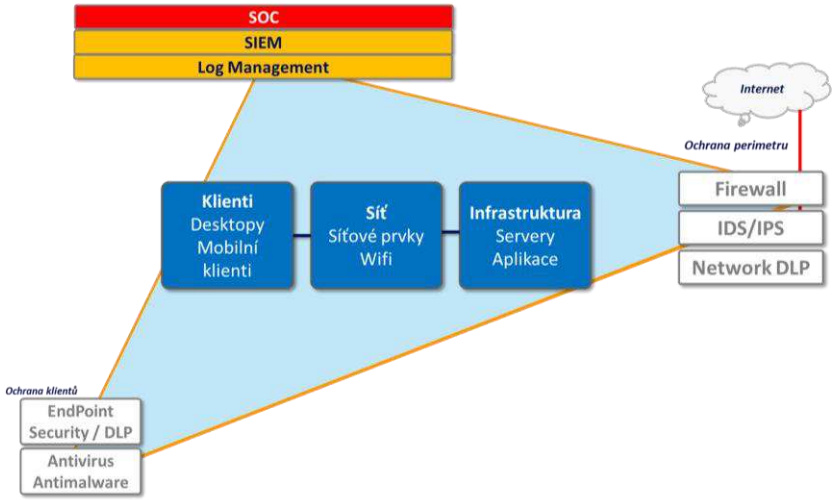


Bermudský trojúhelník bezpečnosti

- **kde? kdo? kdy? jak?**

- **Žádné řízení přístupu do sítě (NAC)**
- **Evidence IP adres v excelu**

Bermudský trojúhelník bezpečnosti

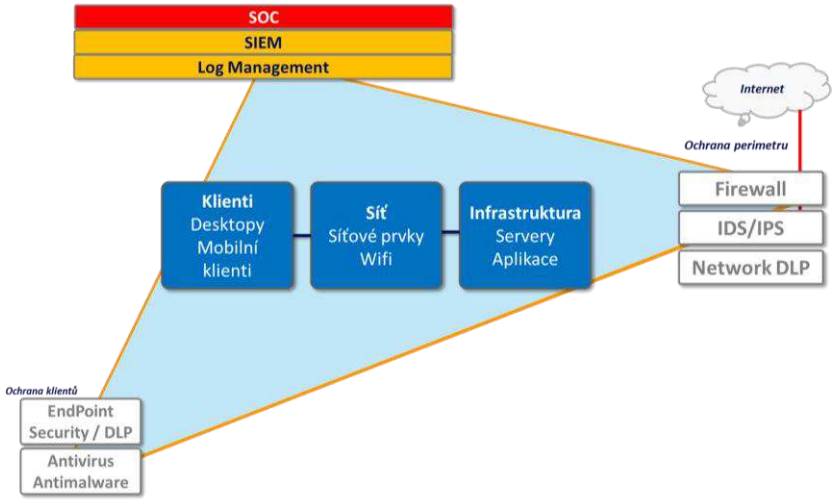


Bermudský trojúhelník bezpečnosti

- **kde? kdo? kdy? jak?**

- **Žádné řízení přístupu do sítě (NAC)**
- **Evidence IP adres v excelu**
- **Dynamicky přidělované IP adresy DHCP**

Bermudský trojúhelník bezpečnosti

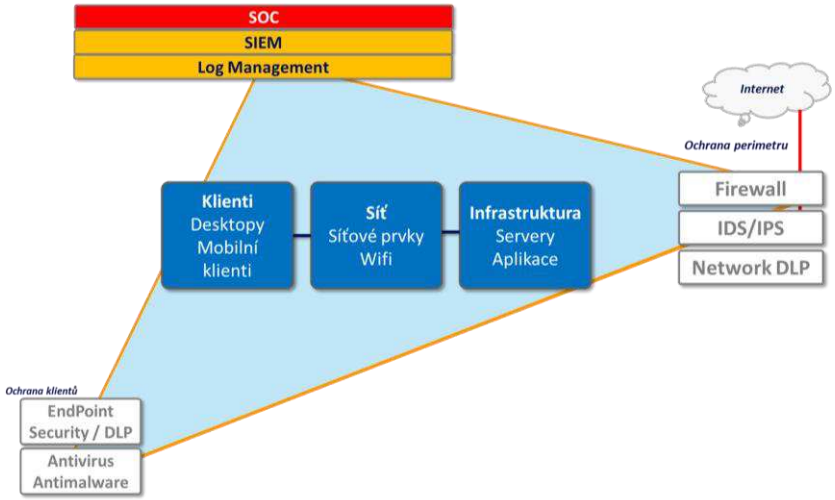


Bermudský trojúhelník bezpečnosti

- **kde? kdo? kdy? jak?**

- **Žádné řízení přístupu do sítě (NAC)**
- **Evidence IP adres v excelu**
- **Dynamicky přidělované IP adresy DHCP**
- **Samostatné DNS**

Bermudský trojúhelník bezpečnosti

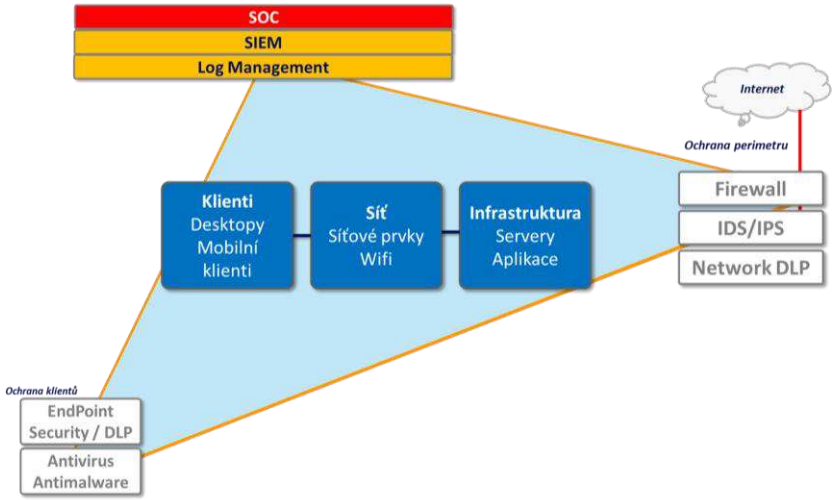


Bermudský trojúhelník bezpečnosti

- kde? kdo? kdy? jak?

- Žádné řízení přístupu do sítě (NAC)
- Evidence IP adres v excelu
- Dynamicky přidělované IP adresy DHCP
- Samostatné DNS
- Pouze základní monitoring
  - Infrastruktura

Bermudský trojúhelník bezpečnosti

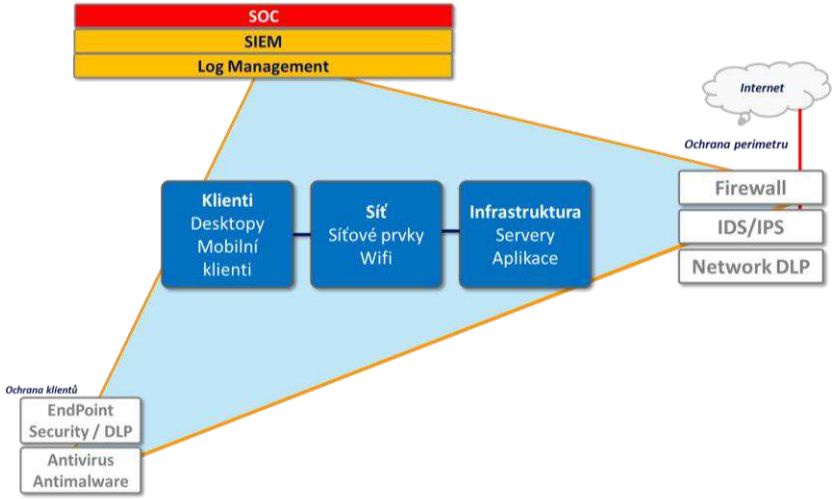


Bermudský trojúhelník bezpečnosti

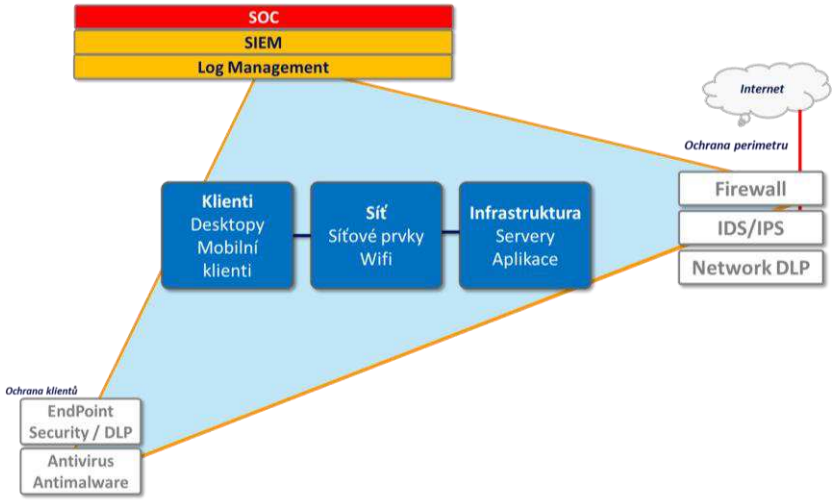
- kde? kdo? kdy? jak?

- Žádné řízení přístupu do sítě (NAC)
- Evidence IP adres v excelu
- Dynamicky přidělované IP adresy DHCP
- Samostatné DNS
- Pouze základní monitoring
  - Infrastruktura
- Žádný pokročilý monitoring síťového provozu

Trojúhelník bezpečnosti



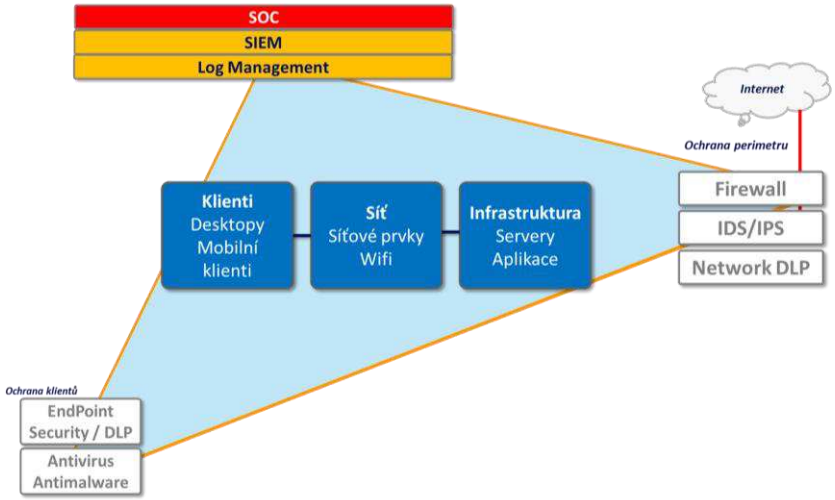
Trojúhelník bezpečnosti



Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

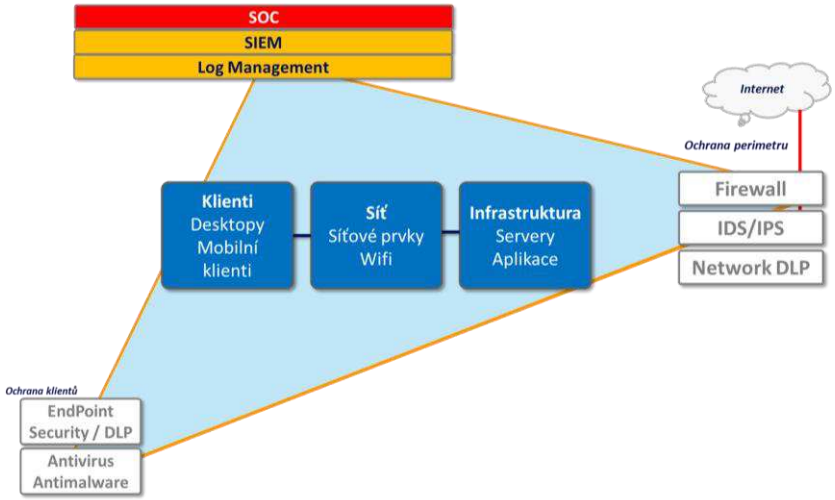
Trojúhelník bezpečnosti



Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

Trojúhelník bezpečnosti

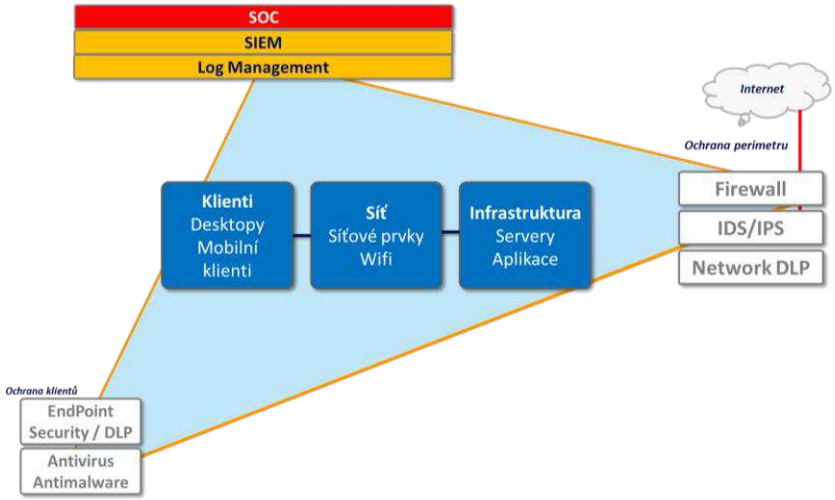


Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

✓ **Řízení přístupu do sítě (NAC)**

Trojúhelník bezpečnosti

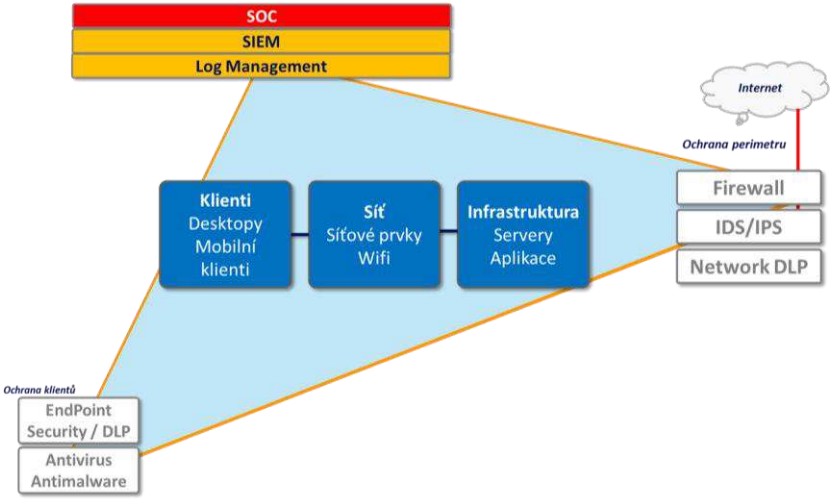


Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

- ✓ **Řízení přístupu do sítě (NAC)**
- ✓ **Pokročilé řízení adresního prostoru (DDI)**
  - ✓ **IPAM, DHCP a DNS**

Trojúhelník bezpečnosti

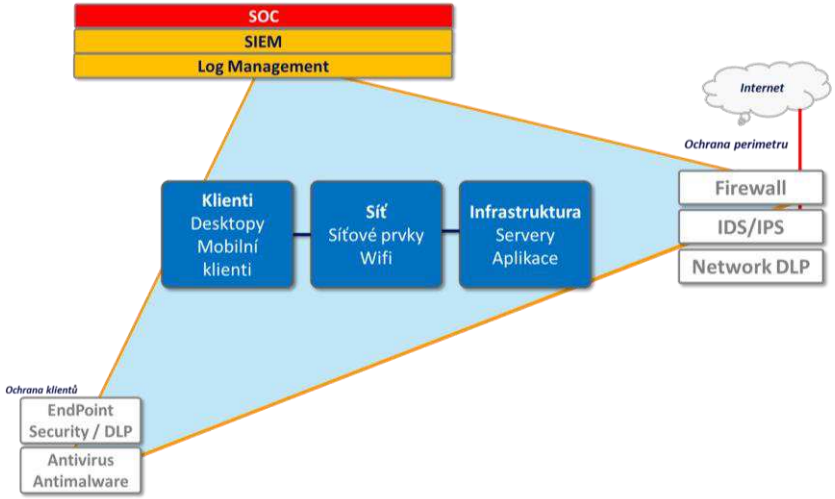


Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

- ✓ **Řízení přístupu do sítě (NAC)**
- ✓ **Pokročilé řízení adresního prostoru (DDI)**
  - ✓ **IPAM, DHCP a DNS**
- ✓ **Pevné IP přidělované DHCP**

Trojúhelník bezpečnosti

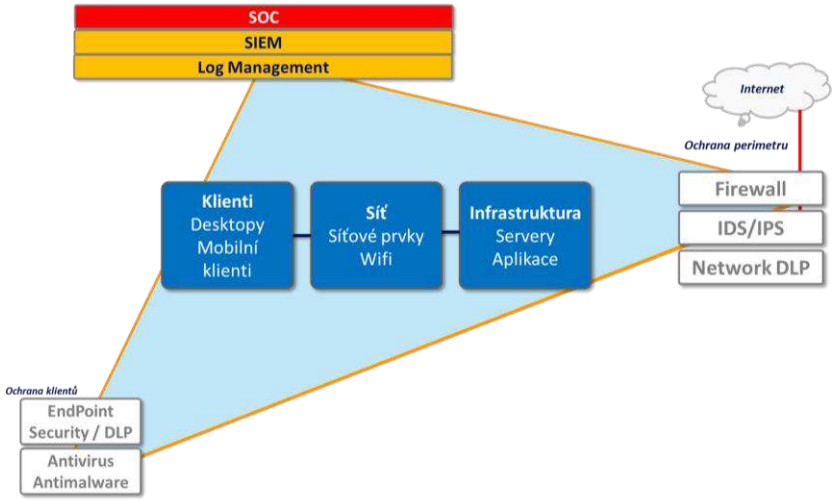


Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

- ✓ **Řízení přístupu do sítě (NAC)**
- ✓ **Pokročilé řízení adresního prostoru (DDI)**
  - ✓ **IPAM, DHCP a DNS**
- ✓ **Pevné IP přidělované DHCP**
- ✓ **Multispektrální monitoring**
  - ✓ **L2 Monitoring, Flow Monitoring, Infrastruktura a aplikace**

Trojúhelník bezpečnosti



Trojúhelník bezpečnosti monitoruji a řídím

- kde, kdo, kdy, jak

- ✓ **Řízení přístupu do sítě (NAC)**
- ✓ **Pokročilé řízení adresního prostoru (DDI)**
  - ✓ **IPAM, DHCP a DNS**
- ✓ **Pevné IP přidělované DHCP**
- ✓ **Multispektrální monitoring**
  - ✓ **L2 Monitoring, Flow Monitoring, Infrastruktura a aplikace**
- ✓ **Pokročilá ochrana vnitřní sítě - NBA**

Konvenční řešení kybernetických incidentů

- **Identifikace hrozby – Operátor SOC**
  - SIEM vyhodnotí bezpečnostní incident
  - SOC operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit

Konvenční řešení kybernetických incidentů

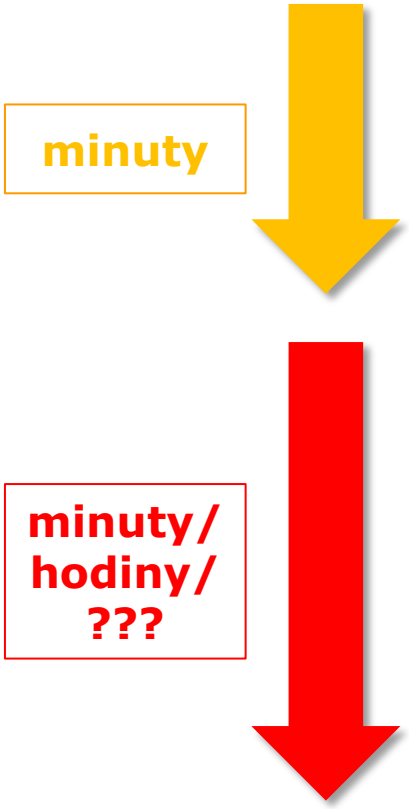
- **Identifikace hrozby – Operátor SOC**
  - SIEM vyhodnotí bezpečnostní incident
  - SOC operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit

Konvenční řešení kybernetických incidentů

- **Identifikace hrozby – Operátor SOC**
  - SIEM vyhodnotí bezpečnostní incident
  - SOC operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit
- **Eliminace zjištěné hrozby - Síťový správce**
  - Převezme z fronty požadavků
  - Začne lokalizovat zařízení
    - dynamická adresa?/ hledání v logách…
  - Přihlásí se na switch a odpojí port
  - Informuje admina PC

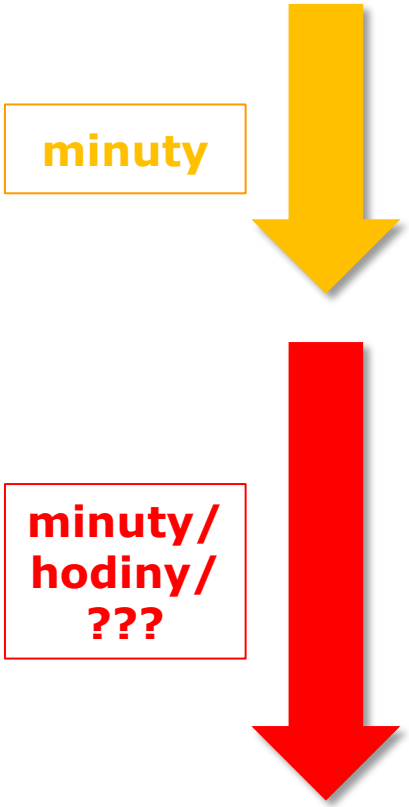
Konvenční řešení kybernetických incidentů

- **Identifikace hrozby – Operátor SOC**
  - SIEM vyhodnotí bezpečnostní incident
  - SOC operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit
- **Eliminace zjištěné hrozby - Síťový správce**
  - Převezme z fronty požadavků
  - Začne lokalizovat zařízení
    - dynamická adresa?/ hledání v logách…
  - Přihlásí se na switch a odpojí port
  - Informuje admina PC



Konvenční řešení kybernetických incidentů

- **Identifikace hrozby – Operátor SOC**
  - SIEM vyhodnotí bezpečnostní incident
  - SOC operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit
- **Eliminace zjištěné hrozby - Síťový správce**
  - Převezme z fronty požadavků
  - Začne lokalizovat zařízení
    - dynamická adresa?/ hledání v logách…
  - Přihlásí se na switch a odpojí port
  - Informuje admina PC
- **Provedení nápravných opatření - Administrátor PC**
  - Vyžádá si fyzické zařízení
  - Provede odvirování
  - Požádá síťaře o znovuzapojení do sítě



Konvenční řešení kybernetických incidentů

- **Identifikace hrozby – Operátor SOC**
  - SIEM vyhodnotí bezpečnostní incident
  - SOC operátor kontaktuje síťového správce
    - Adresa www.xxx.yyy.zzz je infikovaná, odpojit
- **Eliminace zjištěné hrozby - Síťový správce**
  - Převezme z fronty požadavků
  - Začne lokalizovat zařízení
    - dynamická adresa?/ hledání v logách…
  - Přihlásí se na switch a odpojí port
  - Informuje admina PC
- **Provedení nápravných opatření - Administrátor PC**
  - Vyžádá si fyzické zařízení
  - Provede odvirování
  - Požádá síťaře o znovuzapojení do sítě

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
  - případně **změní IP adresu** v integrovaném DDI nástroji

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
  - případně **změní IP adresu** v integrovaném DDI nástroji
  - kontaktuje administrátora PC

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
  - případně **změní IP adresu** v integrovaném DDI nástroji
  - kontaktuje administrátora PC

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
  - případně **změní IP adresu** v integrovaném DDI nástroji
  - kontaktuje administrátora PC
- **Provedení nápravných opatření - Administrátor PC**
  - Vyžádá si fyzické zařízení
  - Provede odvirování
  - Požádá správce sítě o znovupřipojení zařízení do sítě

Pokročilé řešení kybernetických incidentů

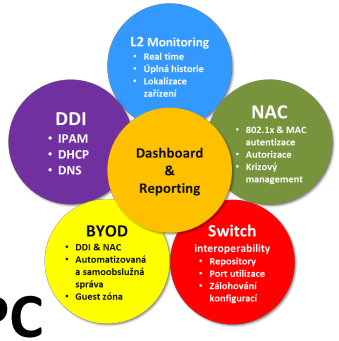
- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
  - případně **změní IP adresu** v integrovaném DDI nástroji
  - kontaktuje administrátora PC
- **Provedení nápravných opatření - Administrátor PC**
  - Vyžádá si fyzické zařízení
  - Provede odvirování
  - Požádá správce sítě o znovupřipojení zařízení do sítě

Pokročilé řešení kybernetických incidentů

- **Identifikace a eliminace hrozby – operátor SOC**
  - SIEM **vyhodnotí** bezpečnostní incident
  - SOC operátor **lokalizuje infikované zařízení** v integrovaném L2 monitoringu
  - SOC operátor **izoluje infikované zařízení** v integrovaném NAC subsystému
  - případně **změní IP adresu** v integrovaném DDI nástroji
  - kontaktuje administrátora PC
- **Provedení nápravných opatření - Administrátor PC**
  - Vyžádá si fyzické zařízení
  - Provede odvirování
  - Požádá správce sítě o znovupřipojení zařízení do sítě

AddNet

minuty



minuty/ hodiny

AddNet

AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů**

AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů**

- L2 monitoringu

AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů**

- L2 monitoringu
- správy IP adresního prostoru

AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů**

- L2 monitoringu
- správy IP adresního prostoru
- základních síťových služeb
  - DHCP, DNS

AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů**

- L2 monitoringu
- správy IP adresního prostoru
- základních síťových služeb
  - DHCP, DNS
- řízení přístupu do sítě (NAC)

AddNet

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

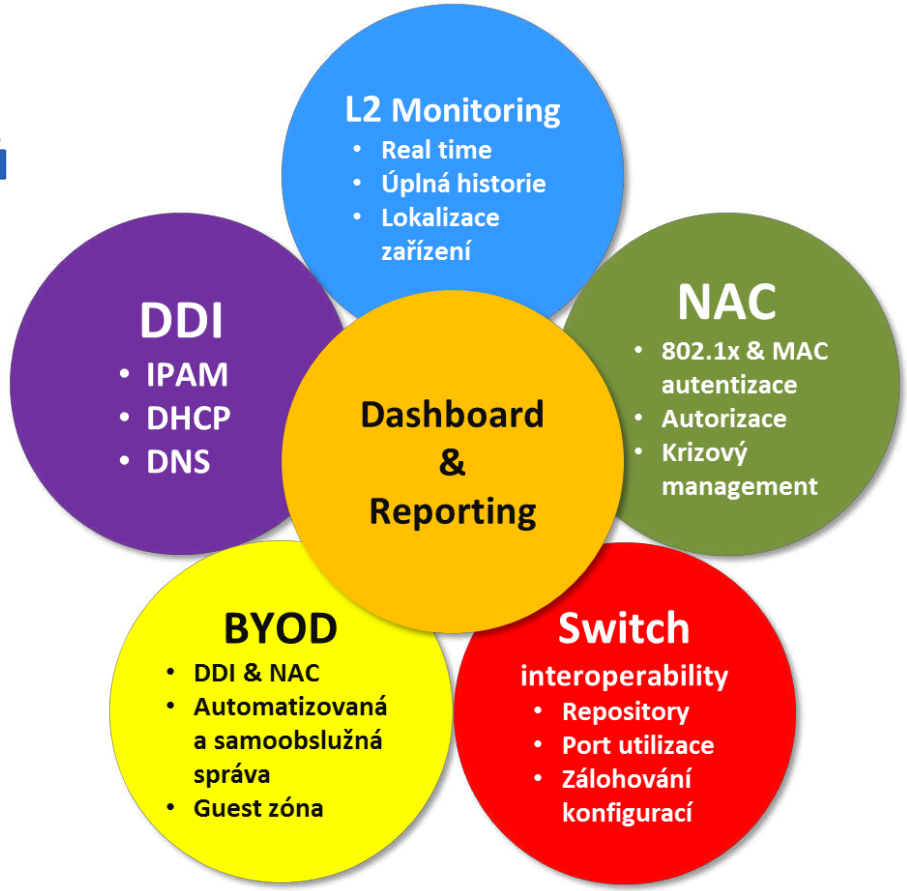
Toho je dosaženo **integrací systémů**

- L2 monitoringu
- správy IP adresního prostoru
- základních síťových služeb
  - DHCP, DNS
- řízení přístupu do sítě (NAC)
- pokročilé komunikace s aktivními prvky sítě

Je unikátní **DDI/NAC nástroj** pro řádové **zvýšení efektivity správy IP adresního prostoru a řízení bezpečnosti přístupu v rozsáhlých sítích**.

Toho je dosaženo **integrací systémů**

- L2 monitoringu
- správy IP adresního prostoru
- základních síťových služeb
  - DHCP, DNS
- řízení přístupu do sítě (NAC)
- pokročilé komunikace s aktivními prvky sítě



Klíčové přínosy AddNetu

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC** – snadné zavedení a správa integrovaného řízení přístupu do sítě
  - 802.1x / MAC autentizace s ochranou a následná Autorizace

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC** – snadné zavedení a správa integrovaného řízení přístupu do sítě
  - 802.1x / MAC autentizace s ochranou a následná Autorizace
- **BYOD** – automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC** – snadné zavedení a správa integrovaného řízení přístupu do sítě
  - 802.1x / MAC autentizace s ochranou a následná Autorizace
- **BYOD** – automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení
- **Zvýšení provozní spolehlivosti DDI/NAC služeb** díky vícenásobné redundanci a nadstandardní škálovatelnosti

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC** – snadné zavedení a správa integrovaného řízení přístupu do sítě
  - 802.1x / MAC autentizace s ochranou a následná Autorizace
- **BYOD** – automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení
- **Zvýšení provozní spolehlivosti DDI/NAC služeb** díky vícenásobné redundanci a nadstandardní škálovatelnosti
- **Úspora nákladů** díky sledování utilizace aktivních prvků

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC** – snadné zavedení a správa integrovaného řízení přístupu do sítě
  - 802.1x / MAC autentizace s ochranou a následná Autorizace
- **BYOD** – automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení
- **Zvýšení provozní spolehlivosti DDI/NAC služeb** díky vícenásobné redundanci a nadstandardní škálovatelnosti
- **Úspora nákladů** díky sledování utilizace aktivních prvků
- **Plná heterogennost -** bezproblémová spolupráce běžnými síťovými technologiemi (včetně Microsoft a Cisco)

Klíčové přínosy AddNetu

- **L2 monitoring** - lokalizace zařízení v síti a úplná historie stavu sítě
- **Řádové snížení pracnosti síťové správy**
- **Standardizace činností a centralizace správy** v rozsáhlých a distribuovaných sítích
- **DDI** – zavedení integrovaných vysoce spolehlivých základních síťových služeb (IPAM/DHCP/DNS)
- **NAC** – snadné zavedení a správa integrovaného řízení přístupu do sítě
  - 802.1x / MAC autentizace s ochranou a následná Autorizace
- **BYOD** – automatizovaná správa a jednoznačná identifikace BYOD a mobilních zařízení
- **Zvýšení provozní spolehlivosti DDI/NAC služeb** díky vícenásobné redundanci a nadstandardní škálovatelnosti
- **Úspora nákladů** díky sledování utilizace aktivních prvků
- **Plná heterogennost -** bezproblémová spolupráce běžnými síťovými technologiemi (včetně Microsoft a Cisco)
- **Snadná implementace** a ověřené projektové postupy

NIM
Novicom Implementation Methodology

Další informace

- **Novicom s.r.o.**
  - Koněvova 67
  - 130 00 Praha 3
  - www.novicom.cz
  - sales@novicom.cz
- **Jindřich Šavel**
  - obchodní ředitel
  - jindrich.savel@novicom.cz
  - +420 271 777 231
  - +420 777 222 961